USAID
FROM THE AMERICAN PEOPLE

DEMOCRATIZING DIGITAL

LANDSCAPE ASSESSMENT

DigitalFrontiers
SCALING DIGITAL DEVELOPMENT

DAI
Shaping a more livable world.

TABLE OF CONTENTS

ACRONYM LIST

AfCFTA	African Continental Free Trade Area
AFR/SD/CPG	Conflict Peace Building and Governance division in the Africa Bureau
AI	Artificial Intelligence
AIRA	Africa Infodemic Response Alliance
APEC	Asia Pacific Economic Cooperation
B2C	Business-to-Consumer
CBPR	Cross-Border Privacy Rules (APEC)
CIPESA	ICT Policy Centre for Eastern and Southern Africa
CPG	Conflict Peace Building and Governance
DCCP	Digital Connectivity and Cybersecurity Partnership
DECA	Digital Ecosystem Assessment
DFS	Digital Financial Services
DIAL	Digital Impact Alliance
DPA	Data Protection Authority
EAC	East African Community
EACJ	East Africa Court of Justice
EALS	East Africa Law Society
ECOWAS	Economic Community of West African States
EGA	Estonia e-Governance Academy
eID	Electronic ID number
EU	European Union
GDP	Gross Domestic Product
GDDF	Global Digital Development Forum
GDPR	General Data Protection framework
GIF	Greater Internet Freedom
GIZ	German development agency
GNI	Global Network Initiative
GoU	Government of Uganda
GPD	Global Partners Digital
GSOD	Global State of Democracy report
ICT	Information and Communication Technology

ID	Digital Identification
ID4D	Identification for Development
IDEA	International Institute for Democracy and Electoral Assistance
IFCJ	International Center for Journalists
LGBTQ	Lesbian, Gay, Bisexual, Transgender, and Queer
LMICs	Low- and middle-income countries
MISA	Media Institute of Southern Africa
MNO	Mobile Network Operator
MOSIP	Modular Open Source Identity Platform
OTI	Office of Transition Initiatives (USAID)
OTT	Over the Top
OU	Operating Units
PATH	Program for Appropriate Technology in Health
PRC	People's Republic of China
PRP	Privacy Recognition for Processors
RAPDP	Network of African Data Protection Authorities
RFP	Request for Proposals
SADC	Southern African Development Community
SDG	Sustainable Development Goal
SMS	Short Messaging Service (text message)
SSA	Sub-Saharan Africa
SSI	Self-sovereign Identity
UCC	Uganda Communications Commission
UPI	Universal Payment Interface
USAID	United States Agency for International Development
VPN	Virtual Private Network
WHO	World Health Organization
ZLHR	Zimbabwe Lawyers for Human Rights

KEY TERMS

Algorithm	An algorithm is a fixed series of steps that a computer performs in order to solve a problem or complete a task. For instance, social media platforms use algorithms to compile the content that users see. These algorithms are designed to show users material that they will be interested in, based on each user's history of engagement on that platform. (Shorenstein Center, 2018) (Disinformation Primer)
Artificial Intelligence	Computer-based automated decision-making, inspired by human-like intelligence. Automated decisions might be directly implemented (e.g., in robotics) or suggested to a human decision-maker (e.g., product recommendations in online shopping). AI often incorporates machine learning (ML), in which predictions are based on patterns "learned" from existing data. (USAID, 2019) Also see Machine learning (Disinformation Primer)
Censorship	The suppression of free speech by governments or private institutions based on the assumption that said speech is objectionable or offensive. In addition to hard forms of censorship (handed down officially through laws and regulations), soft forms of censorship exist (applied through financial and/or reputational pressure). (Digital Strategy)
Civil Liberties	Individual rights protected from unjust interference by governmental or other actors. In the United States, the first ten Amendments to the U.S. Constitution, known collectively as the Bill of Rights, enshrine these rights. Civil liberties include the right to the freedoms of expression and association and peaceful assembly, also recognized as universal human rights under the Universal Declaration of Human Rights. (Digital Strategy)
Civic Space	Safe public spaces, offline or online, in which democratic debate can take place and citizens can freely exercise their human rights, including the freedom of opinion and expression. (Roberts 2021)
Civil Society Organizations	Formal non-government organizations (NGOs), as well as formal and informal membership associations (including labor unions, business and professional associations, farmers' organizations and cooperatives, and women's groups) that articulate and represent the interests of their members, engage in analysis and advocacy, and conduct oversight of government actions and policies. (DRG 2013)
Cyber Sovereignty	The idea that countries should be able to decide how their citizens use the internet, even if countries set rules that violate international norms of free expression and free association. (Feldstein 2020)
Dangerous Speech	Any form of expression (speech, text or images) that can increase the risk that its audience will condone or participate in violence against members of another group. (Disinformation Primer)
Data Localization Laws	Laws that require data to be stored, processed, or handled within the borders of the country where the data originated. Many countries are adopting data-localization laws to avoid surveillance or interference by foreign governments or corporations. At the same time, data-localization laws can leave citizens and businesses with no means to avoid surveillance by the intelligence agencies of their own governments and hinder cross-border flows of data, which can have a negative effect on e-commerce and the development of an open, secure, and inclusive digital ecosystem. (Digital Strategy)
Data Privacy	The right of an individual or group to maintain control over, and the confidentiality of, information about themselves, especially when that intrusion results from undue or illegal gathering and use of data about that individual or group. (Digital Strategy)
Data Protection	The practice of ensuring the protection of data from unauthorized access, use, disclosure, disruption, modification, or destruction, to provide confidentiality, integrity, and availability. (Digital Strategy)
Democratic Backsliding	State-led debilitation or elimination of the political institutions sustaining an existing democracy. (Bermeo 2016)
Democracy	A civilian political system in which the legislative and chief executive offices are filled through regular, competitive elections with universal suffrage. Democracy is characterized by civil liberties, including the rights to speech, association, and universal suffrage, as well as the rule of law and respect for pluralism and minority rights. Democracy means 'rule by the people' wherein the authority of the state is rooted in the explicit consent of its citizens. Following from this basic conception, the extent of democracy in a given society can be considered along three key dimensions: 1) the degree of free contestation for political authority; 2) the extent and character of inclusion in that contestation; and 3) the level of recourse to democratic deliberation based on dialogue and the exchange of ideas. (DRG 2013)

Democratic Governance	Governance that takes place in the context of a democratic political system, which is representative of the will and interests of the people and is infused with the principles of participation, inclusion, and accountability. (DRG 2013)
Digital Authoritarianism	The use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations. (Digital Strategy)
Digital Divide	The distinction between those who have access to the Internet and can make use of digital communications services, and those who find themselves excluded from these services. Often, one can point to multiple and overlapping digital divides, which stem from inequities in access, literacy, cost, or the relevance of services. Factors such as high cost and limited infrastructure often exacerbate digital divides. (Digital Strategy)
Digital Ecosystem	The stakeholders, systems, and enabling environment that together empower people and communities to use digital technology to gain access to services, engage with each other, or pursue economic opportunities. A digital ecosystem is conceptually similar to, but broader than, a digital economy. Although certain aspects of the digital ecosystem have country-wide reach, other features differ across geographies or communities. The critical pillars of a digital ecosystem include the following: (1) sound enabling environment and policy commitment; (2) robust and resilient digital infrastructure; (3) capable digital service-providers and workforce (e.g., both public and private institutions); and, (4) empowered end-users of digitally enabled services. (Digital Strategy)
Digital Hygiene	Routine-based digital practices for individuals and organizations to minimize cyber risks.
Digital Identity System	Digital identification (ID) systems register individuals into a computerized database, often with biometrics such as fingerprints, and in turn provide these individuals with certain credentials (e.g., identifying numbers, cards, digital certificates, etc.) that can be used as proof of identity. (Digital Strategy, modified).
Digital Infrastructure	The foundational components that enable digital technologies and services. Examples of digital infrastructure include fiber-optic cables, cell towers, satellites, data centers, software platforms, and end-user devices. (Digital Strategy)
Digital Literacy	The ability to "access, manage, understand, integrate, communicate, evaluate and create information safely and appropriately through digital devices and networked technologies for participation in economic and social life. This may include competencies that are variously referred to as computer literacy, information and communication technology (ICT) literacy, information literacy, and media literacy." Digital literacy includes both hard skills related to the use of hardware or software and digital soft skills related to the use of digital media and information. (Digital Strategy) (Disinformation Primer)
Digital Repression	Digital repression refers to the use of digital tools and technology to violate human rights and includes five techniques — surveillance, censorship, social manipulation and disinformation, internet shutdowns, and targeted persecution of online users. While digital repression is common under authoritarian regimes, democracies have also used these techniques. Digital repression is not limited to government actors; non-state and foreign actors (including private sector and religious groups) can also deploy these techniques for political, social, and economic reasons. Digital repression can be deployed using various technological tools including surveillance cameras, commercial malware, social media "botnets", and access-blocking firewalls. Censorship and surveillance circumvention technologies (e.g., VPN, encrypted messaging applications) are used by people in many countries to mitigate some elements of digital repression. (DECA Toolkit, forthcoming)
Digital Rights	Human rights in online spaces. These rights include, but are not limited to, the right to privacy, freedom of opinion and speech, freedom of information and communication, gender rights, and the right to freedom from violence. (Roberts 2021)
Digital Security	The practice of understanding one's digital footprint, identifying localized risks to information systems and taking reasonable steps to protect one's owned assets from loss or capture. (USAID, 2019) (Disinformation Primer)
Disinformation	Disinformation is false information that is deliberately created or disseminated with the express purpose to cause harm. Producers of disinformation typically have political, financial, psychological, or social motivations. (Shorenstein Center, 2018) (Disinformation Primer)
Gaslighting	A technique of deception and psychological manipulation practiced by a deceiver, or "gaslighter," on victims over an extended period. Its effect is to gradually undermine the victims' confidence in their own ability to distinguish truth from falsehood, right from wrong, or reality from appearance, thereby rendering them pathologically dependent on the gaslighter. (Disinformation Primer)

Governance	The exercise of economic, political and administrative authority to manage a country's affairs at all levels. It involves the process and capacity to formulate, implement, and enforce public policies and deliver services. (DRG 2013)
Internet Freedom	The U.S. Government conceptualizes internet freedom as the online exercise of human rights and fundamental freedoms regardless of frontiers or medium. The same rights that people have offline must also be protected online—in particular, freedom of expression, which is applicable regardless of frontiers and through any media of one's choice. (Digital Strategy/Disinformation Primer)
Internet Governance	The development and application by governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the internet. (United Nations, 2017) (Disinformation Primer)
Liberation Technology	An optimistic narrative that digital tools would empower citizens to express opinions, mobilize protests, expand the horizons of freedom (Diamond 2010, Feldstein 2020) .
Machine Learning	A set of methods for using computers to recognize patterns in data and make future predictions based on these patterns. Machine learning can be "supervised" or "unsupervised," depending on the level of human oversight. (USAID, 2019) Also see Artificial intelligence. (Disinformation Primer)
Malinformation	Deliberate publication of private information for personal or private interest, as well as the deliberate manipulation of genuine content. Note that these information are based on reality but are used and disseminated to cause harm. (Wardle & Derakhshan, 2017) (Disinformation Primer)
Media Literacy	The ability to methodically consider and reflect on the meaning and source of a post or news article. (Disinformation Primer)
Misinformation	Misinformation is information that is false, but not intended to cause harm. For example, individuals who do not know a piece of information is false may spread it on social media in an attempt to be helpful. (Shorenstein Center, 2018) (Disinformation Primer)
Pink Slime Journalism	A low-cost way of distributing thousands of algorithmically generated news stories, often with political bias. (Disinformation Primer)
Propaganda	True or false information spread to persuade an audience but often has a political connotation and is often connected to information produced by governments. (Disinformation Primer)
State Surveillance	Observing, listening, monitoring or recording by a state or its agents to track citizen's movements, activities, conversations, communications or correspondence, including the recording of metadata (Roberts October 2021)
Surveillance law	The legal framework adopted to enable a state to conduct surveillance on those suspected of crimes. With proper protections built in such as requiring authorization by a judge and other safeguards, surveillance laws can protect privacy rights and avoid arbitrary or mass surveillance. Without these protections, surveillance law is often used to justify state surveillance and the violation of human rights. (Roberts October 2021)
Universal Human Rights	A set of rights inherent to all people regardless of place of birth, nationality, and/or citizenship, as defined by the Universal Declaration of Human Rights, including the rights to life, liberty, and security of person; freedom from slavery and torture; freedom of expression, association, and peaceful assembly; as well as the right to access work and education. (Digital Strategy)

FOREWORD

Digital tools play an increasingly critical role in achieving development outcomes in Sub- Saharan Africa. Mobile money has lifted people out of poverty by making it easier and cheaper to save and send money, while internet access delivers vital health and education services, among others, to remote areas, notably during COVID-19 lockdowns. The immense potential of digital development to accelerate other development objectives is clear and is an emerging priority for USAID. USAID published its first Digital Strategy in 2020 and has developed a host of tools to support digital development.

USAID expects digital development to continue across the African continent to foster the growth of a healthy, inclusive, and resilient digital ecosystem, to enhance the digital economy and infrastructure, to accelerate human capital development, and to strengthen the digital enabling environment.

While the potential for these technologies is far reaching, there is growing recognition that such technologies are also used by governments to repress, censor, surveil, and confuse their citizens. Digital tools can be used to accelerate and scale tactics that undermine the ability of citizens to exercise their basic rights and to hold their governments accountable. Even as citizens and civil society leverage digital tools such as social media and private messaging to communicate, organize, and advocate, governments are innovating just as quickly.

The Conflict Peace Building and Governance division in the Africa Bureau (AFR/SD/CPG) of USAID commissioned this landscape assessment in order to better understand digital repression in Sub-Saharan Africa—from the use of artificial intelligence and facial recognition for mass surveillance to the leveraging of social media algorithms to systematically spread disinformation—and to explore ways to mitigate the potential for these undemocratic uses of technology. There is no easy answer. Yet, it is necessary to ask hard questions to achieve open, inclusive, and secure digital ecosystems throughout the region. Future digital development will require navigating political, technical, cultural, and social complexities.

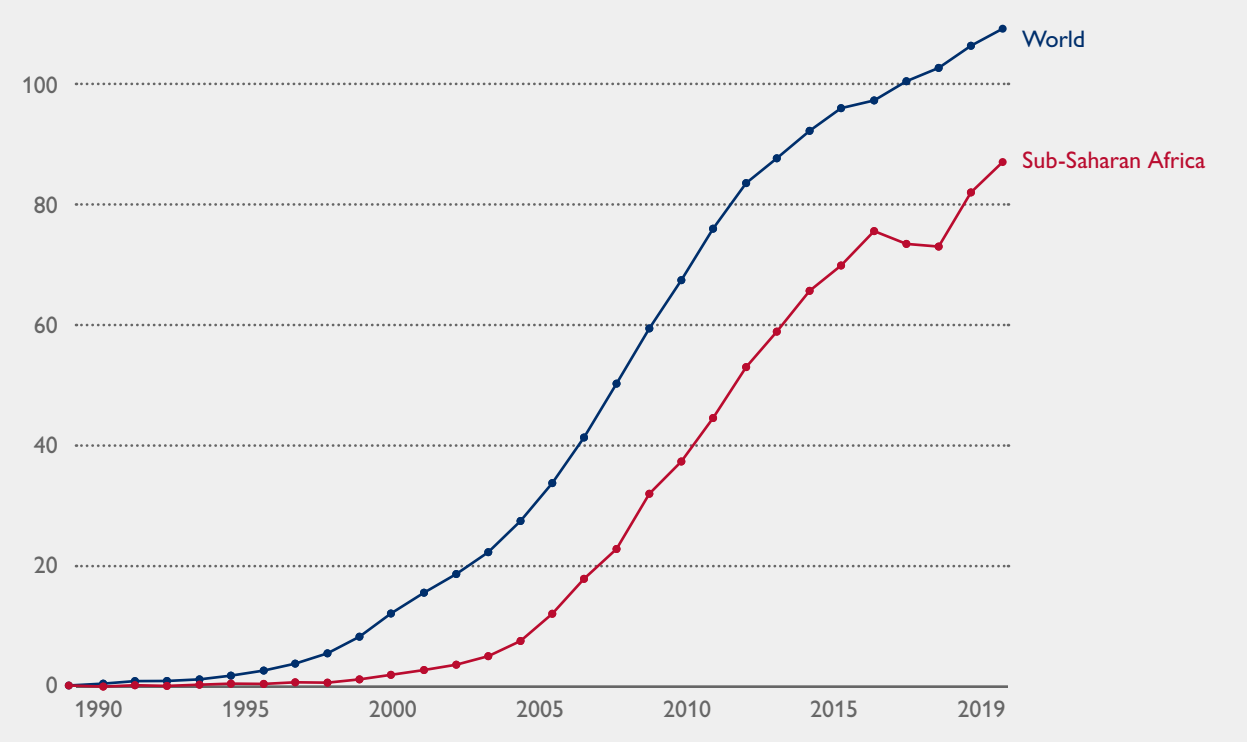
AFR/SD/CPG manages a suite of rigorous, practical, learning-oriented activities to inform Sub-Saharan Africa Mission programming, AFR budgeting choices, and interagency policy decisions. CPG generates and disseminates cutting-edge knowledge and research in the program areas of Peace and Security and Governing Justly and Democratically, with the goal of improving the efficacy and efficiency of USAID programming in Sub-Saharan Africa. CPG activities aim to deepen the knowledge base of best practices, lessons learned, innovations, and new findings in conflict, peacebuilding, and governance, and support Missions in the effective utilization of this knowledge.

Thanks to the main author of this report, Chrissy Martin Meier and to the core team that conceptualized this work and put in hours of time to debate and refine ideas: Kellie Burk (USAID), Christiy Coster (DAI), Sarah Logan (USAID), and Laura Sigelmann (USAID). Connor Mackenzie and Anand Varghese of DAI provided additional input, as did numerous USAID staff in DDI/ITR who contributed time and expertise and laid the groundwork for this discussion.

1. Overview

There has been a rapid and widespread uptake of digital tools by individuals, institutions, and governments over the past two decades, in sub-Saharan Africa (SSA) and globally. In SSA, this digital revolution started with the rapid expansion of mobile phone ownership in the early 2000s (Figure 1) and the slower but just as significant expansion of internet usage over the same period (Figure 2). This allowed for people-centric innovations, driving the creation of new business models, approaches to governance, and solutions to persistent problems in the delivery of essential services including health and education. The mobile-centric nature of SSA's digital growth led to innovations that met the needs of the continent and leapfrogged global technology advancements. The region led the way in mobile money adoption, accounting for over half (55 percent) of the world's 135 million mobile money accounts in 2012.[1]

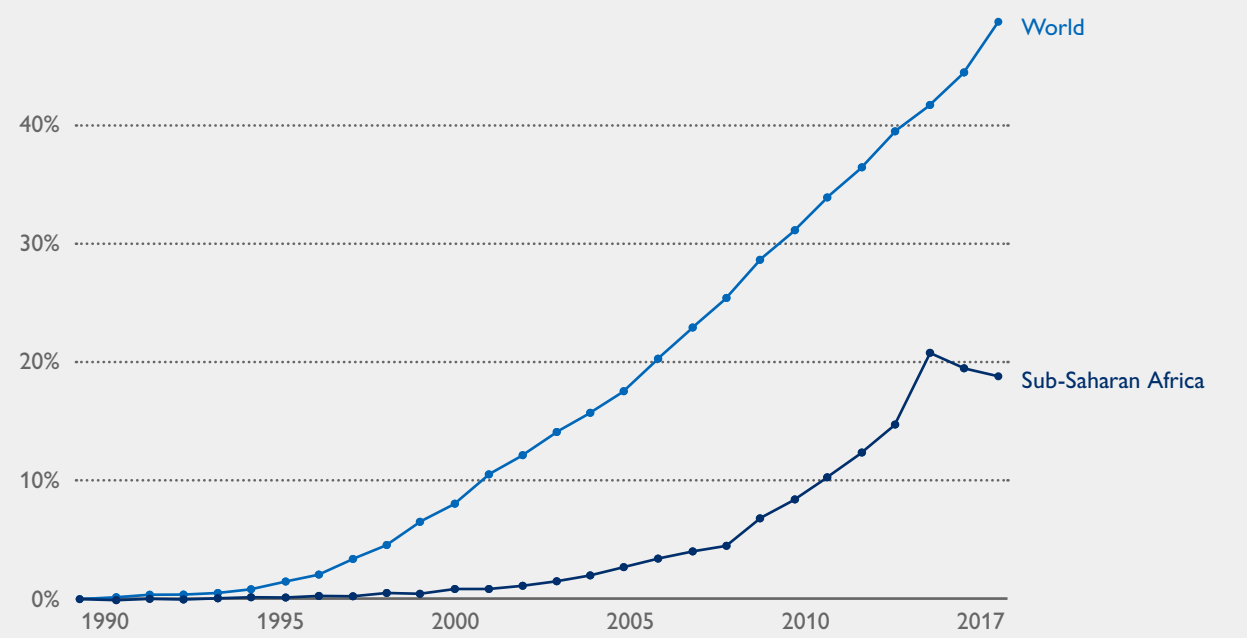
FIGURE 1: Mobile cellular subscriptions per 100 people in Sub-Saharan Africa and the World, 1990 to 2019



Notes: Graph created on February 10, 2022 using OurWorldinData.org.
Source: International Telecommunication Union (via World Bank)

1 Source: GSMA (2017). Global Mobile Money Database, OurWorldinData.org, February 8, 2022. Registered mobile money accounts by region as measured at the end of the year. Mobile money services include transferring money and making payments using a mobile phone, without a formal account at a financial institution.

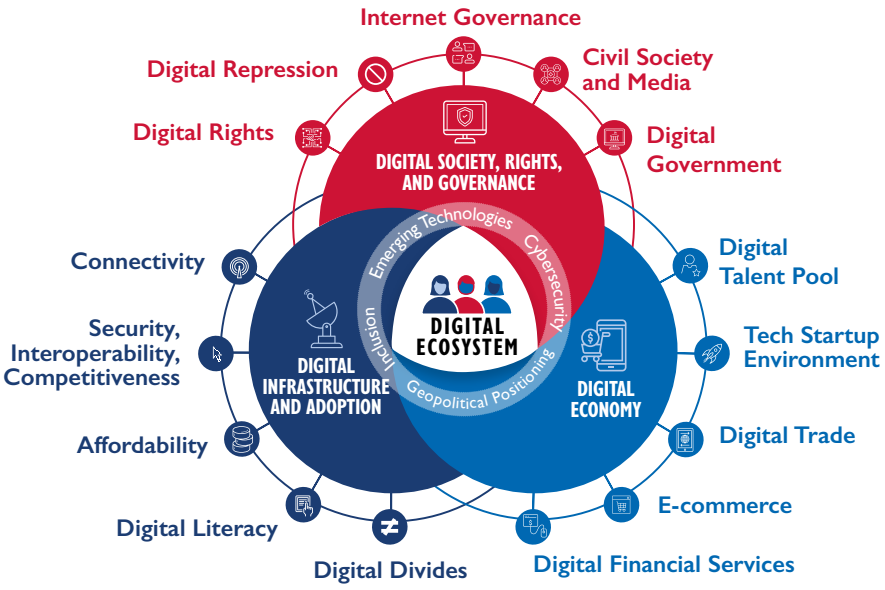
FIGURE 2: Share of population using the Internet, Sub-Saharan and the World, 1990 - 2017



Notes: All individuals who have used the Internet in the last three months are counted as Internet users. The Internet can be used from a computer, a mobile phone, a personal digital assistant, or digital TV, among other sources.
Graph created using OurWorldinData.org on February 10, 2022
Source: International Telecommunication Union (via World Bank)
No explanation provided in dataset for decrease from 2015 to 2017

Digital tools and the *digital ecosystems (Figure 3)* in which they operate today are becoming increasingly complex, creating opportunities and challenges that cross sectors, and requiring new approaches. Governments are adopting new systems for digital identification (ID) and payments; the private sector is driving the uptake of e-commerce and digital financial services; and individuals are using a growing number of social media and messaging apps for communication, news, civic engagement, and entertainment. Digital technology has become more useful and more pervasive than ever, due in part to the COVID-19 pandemic.

FIGURE 3: USAID' Digital Ecosystem Framework



Secure, open, and inclusive digital ecosystems can enable sustainable development. The potential of the digital ecosystem to positively affect many aspects of development—including government transparency and accountability, the strength of civil society, and women's empowerment— is well-documented. Mounting evidence supports the positive impact of digital penetration on development. Research shows that for every 10 percent increase in mobile broadband penetration, an increase of between 0.82 to 1.4 percent occurs in the gross domestic product (GDP) of countries in Africa (Becker 2021). As a result, digital has become increasingly important to international development policies and practices. The Sustainable Development Goals (SDGs) include specific targets for enhancing the use of enabling technology—in particular, information and communication technology—to promote the empowerment of women (SDG 5b); to extend mobile and internet use (SDG 9c); and to expand access to information and communication technologies (ICTs) (SDG 17.6 and 17.8).

USAID has been a leader in digital development for decades. USAID programs focus on expanding access to and using digital technology, and sector-focused programs integrate digital tools to accelerate impact. USAID launched the Leland Initiative in 1996 to bring early internet connectivity to Africa; launched Mobile Solutions Technical Assistance and Research (mStar), a funding mechanism focused solely on digital development, in 2012; led the endorsement campaign for the Digital Development Principles in 2015; and adopted its first Digital Strategy in 2020.[2]

The use of digital technology to boost development impact is referred to as *digital development* in this document. Digital development includes digital health (often referred to as mHealth); digital agriculture (often referred to as ICTforAG); digital education (ICT4E or EdTech); and various efforts related to economic growth and trade, including digital financial services (DFS), the buying and selling of goods online (e-Commerce), and the expansion of underlying digital infrastructure including mobile and internet connectivity, access, and use.

Extensive literature and programming on *digital democracy* cover the ways in which digital tools can impact governance. Referred to in this document as digital democracy, this area of work is also called digital activism and digital governance. Significant energy, research, and funds have been devoted to digital democracy since 2010; several publications focus on the use of digital technology and social media by activist movements behind the Arab Spring. The work shows how digital tools create new spaces for engagement between citizens and the state, offer new opportunities for civil and political discussion and activism, and have the potential to facilitate democratic processes like elections.[3]

Recent literature on digital democracy has shifted focus to the negative potential of digital technologies. While these technologies have empowered civil society and activists by opening new civic spaces, they

BOX 1: Defining digital authoritarianism and digital repression

Digital authoritarianism occurs when a repressive government controls the Internet and uses censorship, surveillance, and data, media, law and regulations to restrict or repress rights at scale.

Digital repression occurs when any actor, including democratic or repressive government, non-state, and foreign actors, use digital tools and technology to violate rights.

Thus, digital repression is an action, while digital authoritarianism describes an overarching approach to governance.

Source: USAID Digital Strategy

2 The Digital Strategy provides examples of ways in which digital technology promotes economic development and country self-reliance (pp 8-12).

3 This paper uses the word "citizens" in lieu of "individuals" to refer collectively to individuals, civil society organizations, and the private sector, entities in a country that do not represent the government or the military. This term is not meant to exclude permanent residents, asylum seekers, refugees, or other groups who do not officially qualify as citizens in their country of residence.

have also provided more opportunities for governments to close offline and online civic space. Digital tools can enable digital authoritarianism, digital repression, and mass surveillance by governments and non-state actors (see Box 1 for definitions). These trends are signaled by the increased use of internet shutdowns, disruptions, and restrictions on access to information during elections and protests, as an example.

This summary document examines the link between digital development and digital repression. The authors reviewed a wide variety of peer-reviewed academic papers, project evaluations, blog posts, and research papers published between 2019 and 2022, focusing on the most recent documentation available. Two workshops were held with USAID staff, and researchers drew on personal experiences working on the intersection of digital ecosystems, development, and democracy. While this paper refers to the available literature when possible, additional analysis is provided to fill in large gaps in the available literature.

Research found that the literature on *digital democracy* is largely divorced from literature on *digital development*. While the literature on digital development has increasingly mentioned the need for data protection and privacy in recent years, there are far fewer mentions of cybersecurity and even fewer mentions of digital authoritarianism, mass surveillance, internet shutdowns and disruptions, disinformation, or risks associated with regime change or democratic backsliding. This is true of USAID program evaluations and research and confirmed by interviews with USAID staff conducted in the process of researching this paper.

As a result, digital development literature—and by extension, programming— risks unintentional promotion of approaches that can facilitate digital repression. Initiatives that have the potential to drive significant development impact—such as encouraging interoperability of digital government systems or providing digital systems to civil society and nonprofits—can enable digital repression if proper risk mitigation and safeguards are not in place.

Research shows that digital repression risks are present in all countries, even those with democratically elected governments. While the literature reviewed often points to a strict dichotomy between democracy and autocracy, the line between these two political systems is increasingly blurred. Institutions associated with democracy exist in authoritarian states, and authoritarian laws that justify authoritarianism and repression exist in countries that claim to be democratic. Tactics like disinformation thrive in countries with democratic elections where more overt control tactics may be off limits.

Digital systems put in place today will carry over when a new government is elected, whether a new government takes power by force, or if the current government undermines existing democratic institutions. Assaults on democracy are increasingly initiated by elected governments, a trend referred to as *democratic backsliding* (Kaufman and Haggard 2021) (see Section 3).[4] Digital tools and systems—whether used by governments, civil society, or other actors—must be implemented with the understanding that the government and its commitment to democratic values may change. Safeguards and mitigation strategies are only effective if they can withstand such changes in government.

Digital technologies, tools, and systems, "are neither good nor bad, but never neutral, and they amplify the power of those that control them" (Schoemaker 2021). Digital repression undermines development objectives by widening existing inequalities, especially those related to income and gender (Section 3). Digital systems, such as digital identification (ID) systems, can drive positive impact under one government while enabling repression under another (Section 4). This paper contributes to the existing literature by

4 See, for example: Walsh, Declan (2021). "The Nobel Peace Prize That Paved the Way for War," NYTimes.com, December 15. https://www.nytimes.com/2021/12/15/world/africa/ethiopia-abiy-ahmed-nobel-war.html?searchResultPosition=1

documenting how development actors can understand and mitigate risks associated with digital repression to ensure that digital development investments drive maximum, positive impact for individuals, societies, and government.

This paper encourages readers to consider potential links between digital development and repression, even when these links have not yet been documented. There are no easy answers, and it is unlikely that available literature will document all risks due to the rapidly changing nature of digital ecosystems and political systems. Two analysis strategies are used in Section 4 to consider which risks may need to be mitigated in digital development initiatives.

Mitigating the risk of digital repression requires amplifying current efforts across governments, civil society, development actors, and the private sector. Preventing the misuse of technology requires creating and adopting technical standards, legal infrastructure, and social and international norms (Section 5). These issues are complex, as digital technology and repression lie at the intersection of development, inequality, geopolitics, security, diplomacy, and the financial interests of many of the world's largest companies. All major global powers are implicated in the spread and use of digital technology for illiberal purposes, thus challenging government-funded donors, including USAID, who can never operate entirely independently from geopolitical interests. Awareness of these issues and a willingness to engage in challenging discussions, starting with asking the questions presented in Section 4, are critical first steps to mitigating the risk that digital investments will be misused. Recommendations for USAID and development partners are presented in Section 6.

2. Key Trends: Digital Democracy and Repression in Sub-Saharan Africa

2.1 THE RISE OF DIGITAL DEMOCRACY

The use of digital technology in democratic movements in Sub-Saharan Africa dates back to at least 2005, when Ethiopian bloggers and online platforms mobilized people in advance of parliamentary elections (Okunoye 2020). In 2008, Kenyan activists used an online crowdsourced map to show SMS and other citizen reports of violence following the 2007 election; this was critical to changing the official narrative and demonstrating the true extent of state-sponsored violence. Citizen journalists turned to social media sites and blogs to report on post-election violence and circumnavigate media restrictions implemented by the government (Makinen and Kuira 2008). The crowdsourced map and proliferation of social media demonstrated the power of open online civic space for activists, even when only 8 percent of Kenyans had access to the internet (Tavaana, n.d.). This opening of online civic space spread quickly beyond Kenya. The Arab Spring uprisings in 2010 and 2011 were a result of citizens taking advantage of newly opened online spaces to protest against repressive governments. In the early days of the Arab Spring, tech-savvy activists gained an initial advantage over the political establishment through creative use of social media to mobilize protestors.

These events generated tremendous enthusiasm for the potential of digital tools to drive a new wave of digital democracy. In 2010, Larry Diamond coined the term "liberation technology" to describe the power of digital tools to allow people to express opinions, organize protests, and "expand the horizons of freedom" (Diamond 2010). In theory, online social media and news platforms can open spaces for civic engagement that are not subject to traditional gatekeepers, such as newsroom editorial boards, intellectual elites, and political parties, thus providing new ways to hold their governments accountable (Menocal 2021).

Activists continue to innovate. The early use of SMS and social media for organizing (popular in the Arab Spring and Kenya examples) continues to grow, and activists are adding new tools, including so-called hashtag campaigns, including global movements such as #MeToo and #BlackLivesMatter, and Africa-specific movements such as #EndSARs in Nigeria. These campaigns use the power of social media to open civic space by allowing diaspora communities to deepen the impact of local activism. The Diaspora helped to ensure that the Cameroon #AnglophoneCrisis went viral internationally. Another recent strategy is the use of virtual private networks (VPNs). Activists and the general public use VPNs to stay online during internet and social media shutdowns. Many have adopted encrypted messaging apps such as Signal and Telegram to avoid censorship and surveillance, (Roberts 2021).

2.2 THE RISE OF DIGITAL REPRESSION

While digital tools have opened new democratic spaces, governments have learned how to use these tools to enable repression. Repressive governments started to adapt almost immediately to the rise of digital activism. Countries not directly affected by the Arab Spring, such as Sudan and Uganda, temporarily blocked SMS and social media sites in their countries after the 2011 Arab Spring uprisings. In his 2010 article, often cited for its techno-optimism, Diamond recognized that autocratic governments were quickly learning to master these technologies (Diamond 2010). This leads to what has been described as a "whack-a-mole" game of governments closing open online spaces nearly as quickly as citizens create them (Roberts 2021).

Research shows that governments are successfully adapting to the risk of digitally-powered protests. As the use of digital repression increases, the chance of protest declines (Frantz, Kendall-Taylor, and Wright, 2020). While digitized government systems have improved service delivery in many cases, these systems have also furthered the ability to control, surveil, and censor in other cases. Governments have effectively weaponized the law to legitimize all of the tactics of digital repression in order to get the upper hand in the ongoing game of whack-a-mole, introducing provisions in laws and policies to allow for the infringement of digital rights, and for the infringement of basic human rights using digital tools (State of Internet Freedom in Africa 2019). As technology advances, digital repression follows. When activists launch hashtag campaigns, governments launch disinformation campaigns to undermine their messages and confuse the general public. When people shift to VPNs to avoid censorship, governments find ways to block them. China and Russia have attempted to implement a ban on VPNs, although VPNs have managed to stay active (Gargiulo 2021).

This paper cites **five overarching tactics of digital repression** as outlined in USAID's Digital Ecosystem Framework and originally defined by Steven Feldstein in his April 2021 book *The Rise of Digital Repression*: (1) surveillance of online and offline activity using digital tools; (2) social manipulation and disinformation; (3) partial or full internet shutdowns; (4) digitally-enabled targeted persecution; and (5) censorship of political speech, both offline and online.

Digital repression tactics can be used by any government or non-state actor to violate human rights. Digital authoritarianism is the systematic use of digital repression by an authoritarian government (see Box 1). This paper focuses on the use of the five tactics mentioned above by governments against domestic populations, as this was found to be a significant gap in existing literature.[5]

The following section outlines relevant technologies, recent use cases, and specific country examples to illustrate trends related to each of these tactics by state actors. These examples are non-exhaustive. The five tactics are not mutually exclusive and in many cases overlap and enable one another. The intention in Section 4 is to provide an understanding of trends in each area in order to examine how digital development initiatives positively or negatively affect these risks.

5 Misuse of digital technology by non-state and foreign actors is more often referred to as cyber warfare than digital repression, and is covered under the literature on cybersecurity. The U.S. Government Digital Connectivity and Cybersecurity Partnership (DCCP), chaired by USAID and the State Department, aims to help partner governments counter "authoritarian regimes [foreign governments] that seek to dominate the telecommunications industry and control digital tools or services that increase censorship and repression." For more information, refer to resources such as USAID's Cybersecurity Primer and the Global Network on Extremists and Technology.

2.3 THE FIVE TACTICS OF DIGITAL REPRESSION

2.3.1 CENSORSHIP

Digital repression enables new ways to censor and suppress individual speech and media as governments seek to control public narrative. A 2021 study found that 43 African countries (of 54 countries in Africa) restrict political media, with 11 exercising heavy censorship. (Comparitech 2021). As with all forms of repression, censorship is not new.

Digital technologies provide new tools to block or ban certain types of speech and intimidate people into avoiding political speech. The other four tactics to be described in this section are used to censor online and offline speech. Surveillance and targeted persecution instill fear of speaking freely; disinformation is used to silence criticism; and internet shutdowns are used "when all else fails." [6] Censorship can also target specific types of online speech, through the monitoring, blocking, or banning of political speech or speech classified as pornography (Comparitech 2021).

Effective digitally-enabled censorship requires resources. Governments in SSA are limited in their ability to monitor and block all online speech due to the financial and technical resources required, unlike China, considered the world leader in internet censorship. These governments rely instead on blacklisting certain websites by providing web addresses to local internet service providers and deleting previously published content (Wilhelm 2018). China has been able to coerce global internet platforms into developing specific products designed to meet their censorship demands, preventing banned information from reaching its citizens (DW 2018).

In the absence of independent resources, SSA countries often import technology from other countries, including China, the United States, and European countries. This gives rise to fears that SSA countries will import data repression tactics along with the technology, particularly from China. While some literature sources worry that China is actively exporting its censorship model and technology in efforts to undermine democracy, other sources claim that this narrative is "oversimplifying a complex environment" and that SSA countries will find the censorship technology they want, regardless of its origin. (Gambardella and Bagwandeen 2021).

There are no easy answers to preventing digitally-enabled censorship, and there is no single country to blame. Preventing censorship, mitigating its effects, and finding ways to reopen offline and online civic space require nuanced and coordinated approaches that reach across the digital ecosystem. Increasing digital literacy encourages individuals to think critically about online information, and bolstering the digital economy and supporting local technology companies mitigates the need to import digital tools. Strengthening internet governance laws and regulations can help civil society hold governments accountable for abuses (Gambardella and Bagwandeen 2021). See Section 5 for examples of mitigation efforts.

2.3.2 SURVEILLANCE

Digitally-enabled government surveillance is a second tactic of digital repression. Governments maintain the need to violate the right to privacy in the name of national security, to

6 In the literature outside of that written by Feldstein, censorship is often used as indistinct from these other tactics. See, for example, "What Internet Censorship Looks Like," NYTimes, January 21, 2021, which discusses internet shutdowns under the aegis of censorship. Available at: https://www.nytimes.com/2021/01/21/technology/internet-censorship-uganda.html. Okunoye 2020 also defines censorship as inclusive of internet shutdowns and online surveillance.

gain advantage during war, or to prevent terrorist attacks.[7] State overreach in the use of surveillance is not new. Colonial powers used surveillance to extract taxes and quell independence movements in SSA and elsewhere through the first half of the twentieth century (Roberts October 2021).

Digital technology has accelerated the use of surveillance at scale, by making it easier and cheaper to monitor communication, and offering new ways to surveil populations. New technologies such as high-resolution cameras, facial recognition, spying malware, and automated text analysis provide copious amounts of data that can be processed and analyzed quickly thanks to artificial intelligence (AI) and machine learning. Governments can survey online discourse to target individuals and to gain insights into opposition, helping governments tap into citizen demands and more quickly preempt discontent (NORC at the University of Chicago and Migliano 2021).

Surveillance data is collected through government-owned technology and through cooperation with or coercion of the private sector. Senegal has purchased FinSpy mobile phone surveillance technology[8] and has made it mandatory for mobile network operators (MNOs) to require all customers to register their mobile phone numbers. This enables governments to gain access to any individual's mobile communications through data requests to MNOs. The Senegalese government has submitted the second-highest surveillance data requests of any country according to transparency reports published by the MNO Orange. (Roberts October 2021).

Foreign governments are selling and donating digital surveillance tools to African governments, both for financial gain and for geopolitical reasons including counterterrorism and securitization. These include the People's Republic of China (PRC), Russia, the United States, and countries within the European Union (EU). Nigeria has spent hundreds of millions of dollars on surveillance technologies procured from Germany, Israel, the People's Republic of China, the United Kingdom, and the United States. (Roberts October 2021).

Efforts are underway in SSA and in countries around the globe to develop, adopt, and implement legal protections (referred to as *surveillance law)* to mitigate the misuse and widespread use of surveillance technology. A recent study suggests that surveillance law on the continent, where it exists, is largely failing to meet this objective.[9] While these laws aim to protect the right to privacy and prevent mass surveillance, in some cases new laws are doing the opposite by explicitly expanding the legal definition of state surveillance. The lack of legal precision and privacy safeguards allows laws to be circumvented. These laws are often ineffective because inadequate capacity in civil society and in the courts allows for state agencies to violate existing law with impunity (Roberts October 2021). While this literature review could not fully examine surveillance law on the continent, the subject warrants further study to understand how current laws are being developed, which provisions are most likely to be abused, and which safeguards are most effective.

7 State surveillance is defined as observing, listening, monitoring, or recording by a government or government-sponsored agent to track a citizen's movement, activities, communications, or correspondence (Roberts October 2021).

8 FinSpy is a commercial spyware program used by law enforcement and government agencies worldwide. This software tricks mobile users into opening a link on their digital device, at which point malware is downloaded onto the device. The malware provides access to the device user's data and activity. For more: https://www.kaspersky.com/blog/finspy-for-windows-macos-linux/42383/

9 Refer to the 2021 report from the Institute of Development Studies on "Surveillance Law in Africa: a review of six countries" for detailed country reports from Egypt, Kenya, Nigeria, Senegal, South Africa, and Sudan. Available at: https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Roberts_Surveillance_Law_in_Africa.pdf?sequence=1&isAllowed=y

BOX 3: The role of legislation in legitimizing digital repression

Governments—regardless of regime type—legitimize digital repression by passing legislation that legalizes specific tactics in the name of national security or rule of law. In some cases, the government's intent that legislation justify repression is blatant, while in others, it is debatable whether legislation is meant to be repressive from the start, or if it is well intended initially and later manipulated by government actors once passed.

Human rights defenders say Kenya's 2018 Computer Misuse and Cybercrimes Act contravenes rights to freedom of expression, privacy, and association. The Act introduced offenses such as publication of false information, cyber harassment, unauthorized interference, and unauthorized interception, which „are phrased so vaguely that it is impossible to tell the conduct targeted by these sections." After civic groups filed a suit, the High Court suspended the implementation of several clauses in the new law due to legal issues in how Parliament and the Senate created the law. Although the case remains in litigation and Parliament is working to address the issues raised by the Court, the Cybercrimes Law was still in force as of March 2021 (Ojango et al 2021). James Wamathai, the Director of Partnerships at the Bloggers Association of Kenya (BAKE), said, "In the past several years, there have been attempts by the government to clamp down on the freedom of expression online. This Act is a testament to these efforts, especially after other sections were declared unconstitutional by the courts (CIPESA 2019)."

2.3.3 DIGITALLY ENABLED TARGETED PERSECUTION

Mass surveillance is linked to a third tactic of digital repression: targeted persecution. Governments have always sought to silence outspoken critics, and now they have new tools to do this. With much of today's political speech and activism occurring online, individuals are creating digital trails for governments to follow through the use of geolocated devices, digital payments, and social media posts detailing location-specific information, all of which can be used by governments to find and arrest citizens (NORC at the University of Chicago and Migliano 2021).

Individuals can be tracked and targeted even when they are not operating online, through facial recognition technology and video surveillance; analysis of this is facilitated by AI. The Zimbabwean government signed a contract in 2018 with the China-based AI company CloudWalk Technology to bring facial recognition software and surveillance technology into the capital city Harare (Chutel 2018). Although the government states that this technology is for monitoring criminal activity, it can also be used to track individuals across the city. Governments use automated text analysis, machine learning techniques, and high powered computing to target individuals and regulate information flows (NORC at the University of Chicago and Migliano 2021).

Governments can exploit legal justifications used to facilitate mass surveillance to legitimize the arrest of online activists (see Box 2). In Nigeria, the Cybercrime Act of 2015 is the major legal basis for surveillance of online bloggers (Okunoye 2020). In Zimbabwe, the Interception of Communications Act of 2007 limits the anonymity of users online by restricting the use of encryption, allowing the government to monitor online activists (CIPESA 2021). The law gives the government jurisdiction to survey mobile phone calls, compelling internet service providers to install surveillance equipment (BBC 2007). In Uganda, the Computer Misuse Act of 2011 outlaws "offensive communication," but has served as a legal basis for silencing online activists who speak out against the government (Musoke 2018). (See Box 3 for more information.)

2.3.4 SOCIAL MANIPULATION AND DISINFORMATION

Disinformation is used by governments and non-state actors to intentionally confuse, undermine, and mislead.[10] Governments may use disinformation to suppress, discredit, and silence opposition (Bradshaw and Howard 2019), or to sow fear and confusion in order to justify repression (Africa Center for Strategic Studies 2021). Disinformation as a strategy exploits the proliferation of ideas as a result of the digital revolution, and more specifically, of social media. While this proliferation was part of the initial excitement around the growth of the internet, it has now given rise to increasingly polarized and rancorous political debate and the tendency of people to consume and discuss news within echo chambers of like-minded people. Disinformation and fake news often directly and intentionally inflame these tensions, and can lead to real life violence (Menocal 2021).

BOX 4: Misinformation, disinformation, and malinformation

	DEFINITION	EXAMPLES
MISINFORMATION	The *unintentional* dissemination of factually incorrect content or information. Spreading factually incorrect content but presented as accurate.	Sharing a news story from a biased media site that contains misconstrued information about a topic.
DISINFORMATION	The *intentional* dissemination of factually inaccurate narratives for political, economic, or other gain.	Fabricated or deliberately manipulated content. Intentionally created conspiracy theories or rumors, often disseminated through widespread campaigns.
MALINFORMATION	The *deliberate* publication of *private information* based on reality for personal or corporate gain rather than public interest.	Sharing the image of a dead refugee child without context to incite a reaction against a specific ethnic group.

Source: USAID Digital Strategy, Kujawski 2019, and authors' own elaboration

The rapid spread of disinformation and fake news is facilitated by political and social factors. A recent study by the Massachusetts Institute of Technology (MIT) found that false information travels on average six times faster than factual news stories, largely because of its ability to shock and awe (USAID Disinformation Primer 2021). This is aided by social media companies who use algorithms to promote stories with more user engagement (often those that shock and awe) while these companies generally struggle to remove disinformation malinformation, and misinformation in a timely manner. This is demonstrated by individuals who have successfully launched disinformation campaigns with scant resources. Six university students at the University of Kinshasa in the Democratic Republic of Congo created a false network of support for a national politician "for the buzz," competing with each other to see who could gain the most followers through posting false information. By the time they were taken down, the fake Facebook pages had amassed 1.5 million Likes (Africa Center for Strategic Studies 2021). A 23-year old in the United States created a satirical disinformation campaign claiming that Birds Aren't Real, a statement on how easy it is to mobilize people around false claims.

10 Disinformation refers to the intentional dissemination of factually inaccurate content for political, economic, or other gain (USAID Digital Strategy, see Box 3).

Disinformation is used by all types of government and "thrives inside of democratic states," where individual leaders and political parties use state-sponsored disinformation when they are not able to employ more draconian methods to exercise or gain power. A recent report by the Oxford Internet Institute found that politicians in 45 democracies have used social media to amass fake followers or have spread manipulated media to garner voter support (USAID Disinformation Primer 2021).

Disinformation is widespread in advance of elections. Incumbent governments use state resources to spread false information against the opposition and political parties routinely hire private companies that specialize in political marketing to profile citizens through their online presence, to spread disinformation, and to foment unrest in the lead-up to elections (Roberts 2021). They also hire troll farms and bot armies as tools to amplify these efforts. Tactics include trolling, harassing, and flooding, often with the intention to deflect criticism and inflate perceptions of regime support (NORC at the University of Chicago and Migliano 2021). Uganda is a prime example of an SSA country using disinformation to influence elections (see Box 3).

Disinformation has numerous adverse consequences. It makes it harder for people to stay informed, undermines trust in democratic institutions, and challenges the ability to engage in online or offline civic discourse. The African Youth Survey, conducted across 14 countries, found that youth in Africa distrust social media as a source of news, with at least 50 percent of those surveyed stating that they do not trust news from either Facebook or WhatsApp - *even though these platforms remain their main source of news* (Africa Center for Strategic Studies 2021).

The line between digital activism and disinformation campaigns is increasingly blurred. While some transnational campaigns are clearly defined as activism (#EndSARS), the same community and diaspora networks can be used to intentionally amplify a government's false and misleading messages. In 2021, the Ethiopian Diaspora set up click-to-tweet campaigns which spread false information denying Eritrea's involvement in the Tigray region, supporting Eritrean and Ethiopian government narratives that justified a military campaign and ongoing ethnic violence perpetrated against the Tigray. This diaspora-led disinformation campaign spread false information— relying on stories from those fleeing the region—by claiming that Western journalists and governments were spreading disinformation in support of the Tigray. The Ethiopian Government joined in this campaign, setting up a Twitter account "Ethiopia Current Issues Fact Check" to warn against trusting the stories of refugees. An internet shutdown in the Tigray (see next sections) facilitated this confusion as people in the region were unable to disseminate video or photo evidence of the actual situation (DFR Lab 2021 and Hale 2021).[11]

There is no single way to mitigate the effects of disinformation. A number of actors are working to find ways to mitigate the worst effects of disinformation (see Section 5). However, current tools are clearly insufficient, as demonstrated by the disinformation campaign launched by Russia in February 2022 to justify its invasion of Ukraine. Russia used false stories generated through artificial intelligence and promoted by recommendation algorithms to frame itself as the victim, denying documented targeting of Ukrainian civilians, and claiming without evidence that the United States provided biological weapons to Ukraine. These stories are spread by official state news sources, state

11 While this paragraph intends to illustrate ways in which disinformation was deployed in advance of the Tigray conflict, it is not a full account of disinformation or digital repression tactics used in relation to this ongoing conflict. Much of the analysis offered here was completed by the Digital Forensic Research Lab (DFRLab) in South Africa, which is part of the Atlantic Council. For more information: https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/

social media accounts, and private users across Facebook, Twitter, YouTube, TikTok, and elsewhere. Russian citizens are denied access to most international media outlets and live behind government firewalls, so they are largely unaware that these narratives are false or even controversial (Paul 2022).

Responses to Russian disinformation by social media companies have been opaque and inconsistent. Disinformation will thrive as long as social media companies value engagement over facts. A study released by the Center for Countering Digital Hate examined a sample of 3,593 articles posted by Russian state news sources in early 2022 and found that Facebook had failed to label 91% of the posts as state-sponsored. Activists have found ways to push back, using digital advertising and direct emails to sneak real news to Russian citizens. This was evolving quickly as of the writing of this report, showing that governments can still control online narratives to justify and enable offline repression, violence, and war in ways previously unimaginable.

2.3.5 INTERNET SHUTDOWNS

Internet shutdowns are used by governments to censor and control, often when disinformation and censorship fail to quash dissent. These tactics are becoming more common. From 2019 to mid-2021, there were 228 major internet shutdowns in 41 countries, creating an accumulated cost to the global economy of approximately $15 billion (NORC at the University of Chicago and Migliano 2021). In 2020, the number of intentional internet shutdowns by African governments rose from 21 to 25 per year, and were often scheduled at the time of elections or popular protests (Roberts 2021).

Internet shutdowns can be complete or partial. Partial shutdowns occur when the government disconnects part of the country, or slows down bandwidth to the extent that use of the Internet becomes nearly impossible (NORC at the University of Chicago and Migliano 2021). In Cameroon, the government shut off internet access specifically in English-speaking regions for 240 days in 2017 during civil unrest (USAID Disinformation Primer 2021). The Government of Mali has shut down the internet partially or fully on a recurring basis since August 2016, when Facebook and Twitter were blocked to quell demands for the release of the columnist Youssouf Mohamed Bathily (known as Ras Bath). Similar social media blocks occurred in June 2017 during a referendum on the constitution and in July 2018 on the day before the first round of presidential elections. The internet was slowed down entirely during the second round of elections (Owono 2018).

The impact of internet shutdowns on human rights and democratic governance is documented, but significant impact on economic development and equality is minimally acknowledged. Internet shutdowns are a violation of human rights with negative social and economic costs, undermining economic growth and eroding business confidence. As noted by the Global Network Initiative (GNI), governments have a legitimate role to protect public safety, but disruptions can have an adverse effect on that very objective, preventing citizen access to vital emergency, payment, and health services, suspending business operations, and cutting off contact among family and friends (CIPESA 2019). A 2016 report by Deloitte estimated that in a country with a developed internet, the per day costs of a shutdown average $23.6 million USD per 10 million people. A country with a less developed internet could experience an average loss of $6.6 million USD per day (Deloitte 2016).

Mitigation requires bringing together individuals and companies to advocate against shutdowns. Public opinion opposes shutdowns. Internet shutdowns can backfire, inflaming tensions and driving people into the streets. They require the cooperation of private companies who comply

in order to maintain access to state-issued licenses in most cases. Mitigation efforts can range from the technical—building in safeguards to ensure that it is not possible for the internet to be shut down—to the political, such as organizing private companies to publish transparency reports and advocate against any type of shutdown (NORC at the University of Chicago and Migliano 2021). See Section 5 for specific mitigation examples.

BOX 5: Digital repression in a Democracy: Uganda as an example of how the 5 tactics are used across SSA

Uganda regularly holds elections and yet is characterized as "not-free" by Freedom House. The government (GoU) has employed all five digital repression techniques with frequency over the past decade, illustrating how these tactics overlap and reinforce one another. Institutions and civil society actors have pushed back against these tactics in different ways, as discussed in later sections. The example of Uganda is used throughout this paper as a way to ground the discussion, highlighting many trends occurring throughout SSA as well as globally, not because it is better or worse than any other country in terms of digital democracy or repression.

The Government of Uganda has *censored* online speech through a social media tax of 500 Ugandan shillings ($.02 USD) per day, significantly decreasing affordability and access in a country with an average income of around $2.00 USD per day. The Ugandan Communication Commission (UCC) has called for online publishers to seek authorization for providing their services, citing Sections 2, 5, and 27 of the Uganda Communications Act, 2013 and Regulation 5 of the Uganda Communication (Content) Regulations, 2019. The need for licenses drives self-censorship and the use of pseudonymous accounts as a platform for speaking out (Freedom House 2021).

Internet shutdowns or disruptions occurred in 2011, 2016, and during Uganda's 2021 Presidential elections (Amnesty International 2021). The most recent internet shutdown took place in the days leading up to the 2021 Presidential election when the government banned multiple social media platforms and news outlets and then enacted a four-day internet blackout while voting took place. The inability to communicate with one another and with those outside the country led to accusations of voter fraud and intimidation, as well as to large economic losses (APC 2021).

Pervasive online *surveillance is,* justified under the RIC Act, 2010, implemented following an al-Shabaab terrorist attack, and the Anti-Terrorism Act, 2002. In 2017, the Uganda Media Centre, a government regulatory body, publicly announced that it had assembled a new social media monitoring unit to identify critical posts. The government has worked with local Huawei employees (a Chinese technology company) to use spyware to access WhatsApp chat groups associated with the opposition, and is now working with Huawei to install a facial recognition surveillance system in Kampala (Freedom House 2021). This surveillance has created a climate of fear that is perpetuated by the *targeting of outspoken individuals*. Stella Nyazi, a popular academic and activist, was jailed for 18 months by the government in 2019 for critical comments she made against the President and First Lady on public Facebook pages (Okunoye 2020). Popular author-poet Kakwenza Rukirabashaija was jailed in December 2021 for posting "offensive" comments about the President's son on Twitter. His arrest was acknowledged by the President of the Poets Association Uganda as a signal that public criticism of the government would not be tolerated (Athumani 2021). The UCC required the registration of social media users in August 2019 (Freedom House 2021).

As of the January 2021 election, the GoU had expanded into *disinformation*. Prior to the election, a network of inauthentic Facebook, Instagram, and Twitter accounts spread coordinated false stories in support of Uganda's ruling party. At least five of the accounts were directly operated by the Ministry of Information and Communications Technology (Africa Center for Strategic Studies 2021).

3. Insights: Digital repression can undermine digital development objectives

All five tactics of digital repression undermine development goals by restricting access to digital tools and spaces. Repression restricts access both directly (through internet shutdowns or media bans) and indirectly (through higher costs and intimidation that lead to self-censorship (Gillwald 2018). Digital repression directly and indirectly increases existing **digital divides** in access and use due to factors such as gender, race, economic status, geography, and disability (DECA Framework). This exclusion hinders the ability of certain groups to participate in the digital economy. As civic and political discourse increases online, digital exclusion hinders the ability to participate in democratic processes.

There is some literature on the impact of digital repression on digital inclusion, specifically for low-income individuals and women. However, further research is needed to understand how digital repression excludes certain groups of people and prevents them from sharing in the positive impact of digitization. The following sections provide a brief overview of the existing literature in order to encourage more research and conversation on the connection between digital repression and digital inclusion.

3.1 LOW-INCOME INDIVIDUALS

Digital repression can intentionally or unintentionally increase the cost of internet and mobile access. Digital repression increases existing digital divides and undermines the ability of the digital ecosystem to deliver equitable development outcomes. When individuals cannot afford mobile devices or access to the internet, they have no access to health, agriculture, or education content, and they cannot advance their digital skills or participate in the digital economy.

Internet shutdowns cost the global economy an estimated $5.5 billion in 2021 (inclusive of social media shutdowns and bandwidth throttling). Nigeria experienced the most significant impact in SSA, losing an estimated $1.5 billion following the government's decision to block Twitter in June

2021 (Hamilton 2022). Some 486 million people were affected globally, meaning that they were unable to participate in online civic discussion or in productive online economic activities such as e-commerce.[12]

Uganda's experience illustrates how digital repression can result in diminished access to vital digital services. On May 30, 2018, Uganda's parliament passed a widely opposed amendment to the Excise Duty Act, introducing an excise tax of Uganda Shillings (UGX) 200, (equivalent to $0.05 USD) per user per day for use of Over the Top (OTT) services such as WhatsApp, Facebook, and Twitter. Three months after the tax was introduced, the number of internet users in the country had declined by 5 million, cutting the internet penetration rate from 47 percent to 35 percent. In the same law, a 0.5 percent tax was imposed on all mobile money cash withdrawal transactions, an issue that has generated public outcry and undermined financial inclusion for those who rely on mobile money for income, including mobile money agents, and for access to services such as domestic remittances and small loans. **The consequences were strongest for those who were already marginalized:** 66 percent of Persons with Disabilities reduced their use of social media with introduction of the OTT tax, while 26 percent of Persons with Disabilities stopped using social media entirely (CIPESA 2019).

3.2 WOMEN

As mobile phones and internet access has expanded across SSA in recent decades, access did not spread equally. Women remain less likely than men to own mobile phones or to have access to the internet, reinforcing existing socioeconomic disparities between genders (USAID Gender Primer 2020). The gender gap in SSA, as measured by mobile internet use, has remained largely unchanged in recent years (37 percent), while the gap across low- and middle-income countries (LMICs) has decreased from 25 percent in 2017 to 15 percent in 2020. Women who are aware of the mobile internet but do not use it report that the main barriers they face are lack of digital skills, the cost of a device, and the cost of mobile internet use (GSMA Connected Women 2021).

Digital spaces are less open to women due in part to their cost. Affordability is a main driver of the persistent gender divide due to structural issues that lead women to have less access to education and income, the primary determinants of mobile access and use (Gillwald 2018). As a result, women are disproportionately affected by the cost issues described in the previous section. Women are adversely affected by digital repression for other reasons, as well.

Compounding affordability issues, all five tactics of digital repression make digital spaces less safe for women because of their gender. Women are more likely to be targeted through the five tactics of digital repression, including disinformation and misinformation (USAID Disinformation Primer). Studies have shown that women journalists experience more attacks and online trolling for their writing than men do for writing on similar topics. In a survey by UNESCO and the International Center for Journalists (IFCJ), 73 percent of female journalists who participated said they have experienced online violence in the course of their work (UNESCO 2020). As a result, women are more likely to self-censor in the face of censorship, surveillance, and targeting, and female

12 Prior to the COVID-19 pandemic, the business-to-consumer (B2C) e-commerce market in Africa was forecast to generate $18.2 billion in 2020. Source: https://www.intracen.org/uploadedFiles/intracenorg/Content/Publications/B2C-marketplaces-20201221_final_Low-res.pdf

journalists are more likely to use pseudonyms or to stop writing on a topic due to the physical and emotional stress caused by harassment (OSCE 2019).

Excluding women from digital spaces limits their ability to participate in the economy and in democratic processes. Access to digital civic spaces has been shown to enable women's empowerment, even where their voices are systematically marginalized. A 2020 study of female youth in rural South Africa showed that females who were encouraged to use digital media to voice societal issues demonstrated changes in their levels of empowerment (Makananise and Madima 2020).

Closing the gender divide requires preventing and mitigating the impacts of digital repression. Censorship, harassment, and targeted persecution can create a culture of fear that undermines the ability of women to participate in digital spaces that support outcomes including health, education, and food security. More data and evidence must be collected on the link between each digital repression tactic, and closer coordination between those working on digital democracy and gender experts is essential. For more on mitigation, refer to Sections 5 and 6.

4. Analysis: Identifying digital repression risks in digital development

Digital repression can undermine development. Can development funding also enable digital repression? This question is not addressed in existing literature. An understanding of digital repression (Section 2) and its impact on development (Section 3) suggests that digital development may unintentionally enable digital repression. This section draws on existing literature to illuminate that potential, using two analysis strategies. This allows for preliminary analysis of risks based on current literature, while setting the stage for more robust research into these links to fill the existing evidence gap.

This section uses two analysis strategies to understand the impact digital development can have on digital repression, drawing from what is known about trends in each area. It encourages an analysis of digital development investments through a *future lens* that accounts for the reality of the global trend toward democratic backsliding. It also offers a high level analysis on how the key digital development trends described in section 1 can affect the ability of governments to use the *five tactics of digital repression*. These analyses inform the selection and implementation of mitigation strategies reviewed in Section 5.

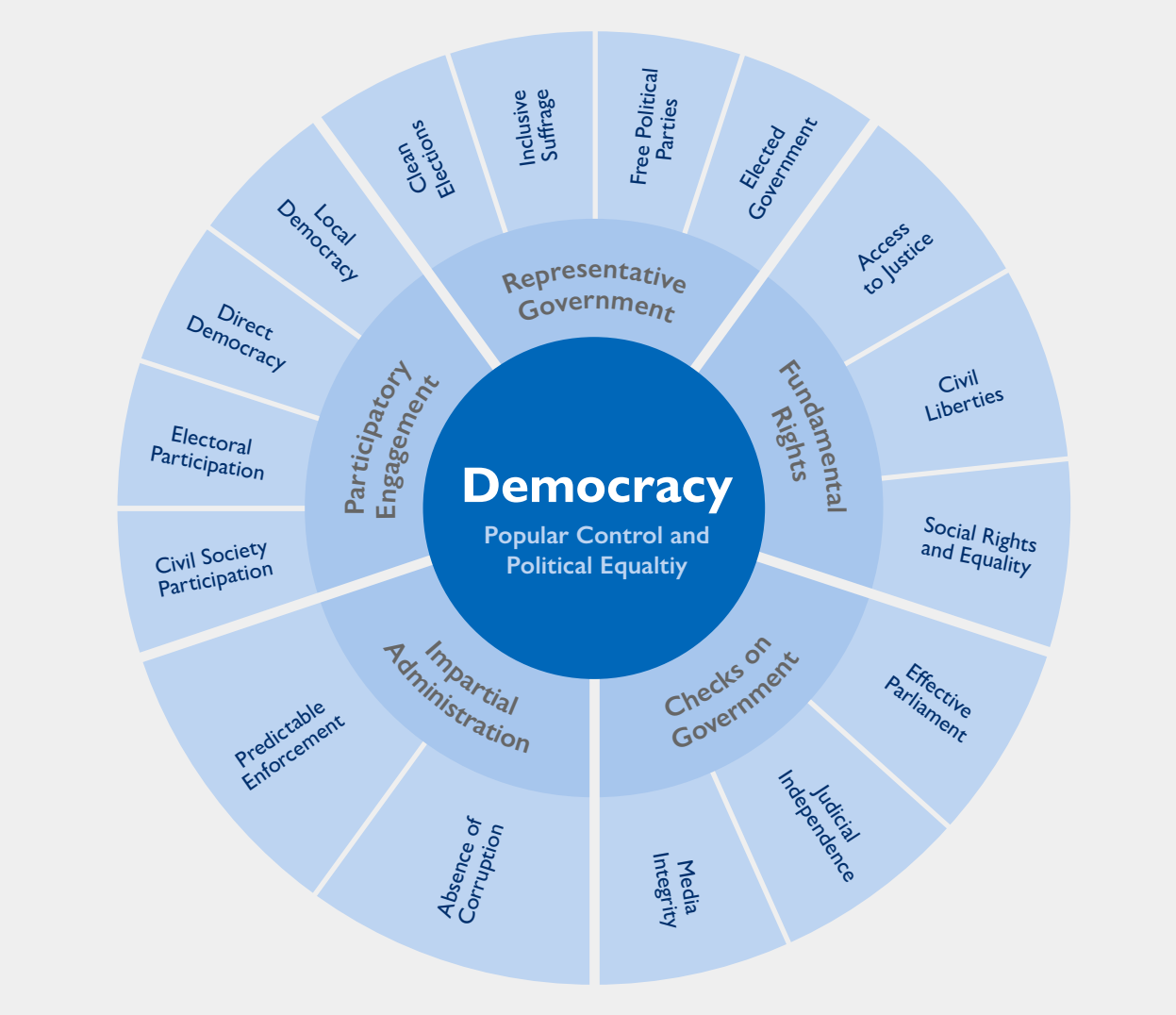
4.1 FUTURE-ORIENTED ANALYSIS

The increasing prevalence of digital repression— both globally and in SSA—aligns with the global trend of *democratic backsliding* in recent years. In countries that are experiencing democratic backsliding, democratically elected governments are working systematically to dismantle democratic processes and institutions. As of 2020, 43 percent more democracies around the world had experienced democratic backsliding than in the previous five years (IDEA 2021).

Understanding and measuring democratic backsliding is increasingly critical to efforts to promote positive digital development and digital democracy. International IDEA's Global State of Democracy (GSoD) has created a tool that measures the state of democratic governance in a country, based on 28 aspects of democracy (Image 4). Using this measurement tool in 168 countries, IDEA estimates that 70 percent of the global population now lives in countries with authoritarian regimes or which are democratically backsliding (IDEA 2021).[13]

13 The IDEA report defines a democracy as a country which, at a minimum, holds competitive elections in which the opposition stands a realistic chance of gaining access to power. Democracies are ranked as weak, mid-range performing, or high-performing. Authoritarian regimes do not hold competitive elections and provide limited to no space for civil society and media. Hybrid regimes do not hold competitive elections but provide some space for civil society and media. IDEA 2021, pp x.

IMAGE 4: Aspects of democracy used to identity democratically backsliding, IDEA 2021



This framework allows for a more nuanced understanding of the state of governance in a country and is more useful to understanding risks. Due to democratic backsliding, the over-simplified black-and-white distinction between democracies and authoritarian regimes is less and less useful. Using this measurement framework, IDEA encourages assessment of the directional state of governance. Is a country moving in a democratic direction or in an authoritarian direction?

The IDEA framework shows that more countries in SSA have moved in an authoritarian direction in recent years. Since 2016, IDEA estimates eight instances of countries in SSA moving in an authoritarian direction: Niger and Zambia in 2016; and Benin, Côte d'Ivoire, Mali, Cameroon, Zimbabwe, and Democratic Republic of Congo in 2020, while finding just three instances of countries moving in a democratic direction: the Democratic Republic of Congo in 2019, and The Gambia and Zambia in 2021.

The IDEA framework provides the first analysis strategy for understanding potential links between digital development and digital repression. In countries moving in an authoritarian direction, digital repression risks can change rapidly, and **it may not be possible to**

predict future risks based on past experience. This analysis asks three questions to assess the potential impact of a digital investment on digital repression:

1. What are the potential misuses of this technology under the current government?
2. What are the potential misuses of this technology if this government begins or accelerates a process of democratic backsliding that undermines any one of the 28 measures of democratic governance?
3. What are the potential misuses of this technology if a new, more authoritarian government takes power?

BOX 6: Afghanistan's digital government systems enable digital repression after regime change

In August 2021, Afghanistan's democratically elected government fell to the Taliban. Upon taking control of the country, the Taliban talked about using the donor-funded digital ID system, e-Tazkira, to target those whom they considered enemies or threats. The Taliban also gained access to other digital government databases supported by donors, including the Afghan personnel and pay system that was used to pay the army and police, containing a ready-made list of potential political opponents. The databases had not developed a key privacy-by-design feature that offers the ability to delete user data (Schoemaker 2021).[14] Thus, systems that had been funded by donors to support coordination and efficiency in a young democracy are now supporting those same objectives—coordination and efficiency—for an authoritarian regime with stated policies of repression and violence against women and political opponents.

4.2 DIGITAL REPRESSION RISK ANALYSIS

How might development funding enable or prevent digital repression? The future-oriented analysis strategy offers one way to consider this question. A risk matrix is a second strategy, as it helps to brainstorm and visualize risks on one table and can be updated as the understanding of risks changes. For the purpose of this paper, we use a simple table that maps a program's objectives to the five digital repression risks (Table 1). The table is further explained as it is used in the analysis throughout this section.

TABLE 1: Risk matrix for visualizing potential links between a development program and the five digital repression techniques

	DIGITAL REPRESSION TECHNIQUES: Objectives might increase risk of… →				
PROGRAM OBJECTIVES: ↓	**Surveillance**	**Disinformation and social manipulation**	**Internet shutdowns**	**Targeted Persecution**	**Censorship**
Objective 1					
Objective 2					
Objective 3					
Objective 4					
……..					

14 Considerations for Using Data Responsibility at USAID states: "In general, you should collect the minimum possible amount of sensitive information, limit the extent to which these data are copied or moved, and delete them once you no longer need them." See also, Governing ID: A framework for the Evaluation of Digital Identity (2020) which points to the ability to delete user data as part of the practice of data minimization.

The two analysis strategies used in this paper discuss trends in digital development as they connect to digital repression, even though these links are largely undocumented in current literature. The following section provides a high level overview of trends in digital government, with a focus on digital identification (ID) and connected digital databases, referred to as government interoperability. An illustrative version of the risk matrix is presented for each one, informed by the three future-oriented questions. The objective is to show how these issues can be considered at a high level, understanding that an accurate risk matrix requires analysis of a specific program in a specific country context.

4.2.1 TRENDS IN DIGITAL GOVERNMENT

***Digital government* refers to the use of digital technologies as an integrated part of government strategies.** It relies on leveraging a country's digital ecosystem to engage government actors, non-governmental organizations, businesses, civil society, and individuals to support the production of and access to data, services, and content through interactions with the government. Digital government can be divided into three broad categories of systems, used by governments to manage, deliver, and engage.

The USAID Digital Government Conceptual Model (unpublished) describes how governments and their development partners are currently investing in the components and processes necessary to advance digital government. According to this model, investments in digital government have the potential to help government agencies become more:

- **Coordinated,** by providing the systems and tools necessary for government bodies to work together across ministries and levels (e.g. national, provincial, municipal);
- **Efficient,** achieving fiscal savings and allowing for innovation by decreasing the time spent on administration;
- **Resilient,** supporting response to and recovery from natural disasters or other sudden social and economic changes;
- **Responsive,** increasing the ability to anticipate and respond to a range of stakeholder needs, including individuals, private sector, and civil society actors.

The model recognizes that in many countries—whether they are classified as democratic or as authoritarian—these objectives may increase government efficiency on the one hand while increasing opportunities for digital repression on the other hand.

To better understand how digital government investments may already or in the future facilitate digital repression, our analysis uses the five techniques of digital repression against the overlay of the four digital government objectives (Table 2). A simple color scheme can be used to show (1) the potential for increasing opportunities for digital repression (red), (2) a neutral impact (orange), and (3) the potential for mitigating or blocking opportunities for digital repression (green). The following sections will apply this analysis tool to two trends in digital government investments: digital ID and interoperability.

TABLE 2: Analyzing Digital Government investments in terms of their impact on digital repression techniques

	DIGITAL REPRESSION TECHNIQUES: Objectives might increase risk of…→				
DIGITAL GOVERNMENT OBJECTIVES: Government can become more… ↓	**Surveillance**	**Disinformation and social manipulatioN**	**Internet shutdowns**	**Targeted Persecution**	**Censorship**
Coordinated					
Efficient					
Resilient					
Responsive					

Digital ID

The roughly 1.1 billion people who lack an official identity are "invisible, discounted, and left behind."[15] Identity unlocks access to formal services as diverse as voting, registering a business or other asset, enrolling in school, opening a bank account, and maintaining health records over time (USAID 2018). The right to a legal identity is enshrined in SDG 16.9, "by 2030 provide legal identity for all including free birth registrations." Development agencies including the UN, World Bank, USAID, GIZ, and a wide variety of foundations have financed or otherwise supported countries in developing digital ID platforms over the past several years. The World Bank has provided support to 25 countries in SSA through its Identification for Development (ID4D) initiative.[16]

Digital development literature is confident that digital ID benefits outweigh the risks. At the same time, the literature regularly emphasizes that there are risks to digital ID which should be mitigated by data protection frameworks and privacy-by-design principles. Two of the 10 2021 Principles for Identification on Sustainable Development focus on security and rights, including "protect privacy and agency through system design" and "protect personal data, maintain cybersecurity, and safeguard people's rights through a comprehensive legal framework."

15 USAID website: https://www.usaid.gov/digital-development/digital-id

16 Full list available at: https://id4d.worldbank.org/country-engagement

BOX 7: Spotlight on: Designing Secure Digital ID Systems

There is no single widely accepted way to design a useful and secure digital ID system. The principles cited above offer general guidelines, while the World Bank and Good ID websites provide a large number of reports and resources. USAID has produced research and guidance of its own. Many of these resources encourage developing countries in SSA and elsewhere to adopt *foundational ID systems*—usually one government-owned ID system which supports access to a wide variety of services. ID systems in the United States and European countries are largely fragmented, where multiple, *functional ID systems* originally designed to access one service (for example, a driver's license which is designed to permit a person to drive) are used to access a variety of services. For more on the design of digital ID systems, refer to the links above.

Best practices suggest that digital ID data can and should be stored in a *decentralized* manner, so the personal data of all citizens is not stored in one central database. Interviews conducted in 2020 with key experts did not uncover a single example of a national government-owned digital ID platform in sub-Saharan Africa, donor-funded or otherwise, that stores data in a decentralized manner. India's Aadhaar, Nigeria's national ID (NIN), and the development donor-funded open-source platform MOSIP are examples of centralized ID databases (Hersey 2021)

Available technology supports a more decentralized approach to identity. One way to create a decentralized system is through the use of blockchain technology. Blockchain can enable self-sovereign identity (SSI), an approach to identity management that stores an individual's personal information on their own device (for example, a card or a cellphone) rather than in a central database. While this approach promises to make it more difficult for non-state or state actors to gain access to and misuse personal data at scale, research suggests that these systems still require robust legal protections and a high level of digital access and literacy (Crumpler 2021).

Another way to decentralize identity data is through federated identity**.** In a federated system, one or more identity providers store personal user data. When a government agency or private company wants to check a person's identity (for example, to ensure that they are the intended recipient of social assistance), that institution's system can check the identity digitally through a secure connection with the identity provider. **No data is transferred,** thus mitigating the risks associated with data-sharing. This concept is now being adopted by some governments in SSA who plan to store identity data separate from civil registration data (records of births and deaths), rather than storing all personal data in one database.[17] Through a secure connection, a record in the identity database (which contains details such as name, age, and address) can be checked against a record in the civil registration database.

Risk is mentioned far more frequently in literature focused on digital democracy, human rights, and activism than in literature focused on digital ID. Digital ID initiatives have been accused by both domestic and foreign governments of directly aiding surveillance and targeting individuals, including the inference that Western countries use these systems to track and target potential refugees and asylum seekers in order to stem migration flows (Privacy International 2020). India's celebrated Aadhaar digital ID system has been accused of starving and killing people (New Yorker 2018 and Guardian 2019, respectively.)

Uganda offers an example for understanding the potential benefits and challenges of digital ID systems. The GoU established a national digital ID system in 2014. By law, all citizens ages 16 and above are required to register for a National ID, at which point their demographic and biometric data is captured and stored in a database maintained by the National Identification and Registration Authority (NIRA). National IDs allow people to vote, to prove eligibility for government programs, to open mobile money and bank accounts, and to obtain access to credit. They also allow

17 Author's personal knowledge of discussions underway in countries in SSA, including Malawi.

the government to ensure that all mobile SIM cards are registered in the country. This has been listed as a benefit in some literature, as it contributes to "security and trust of mobile phone transactions" (RAN Lab 2019, 34). In a USAID-supported survey in 2019 of 2,283 ID holders, registration of SIM cards was cited as the top benefit of ID ownership (68.9 percent). However, Freedom House cites government-mandated registration of SIM cards, especially tied to a biometric ID database, as a key enabler of digital repression, prohibiting anonymous communication which can be vital to civic discourse and allowing for government surveillance and targeted persecution of individuals (Freedom House 2021).

The literature does not tell us whether the benefits outweigh the risks of a digital ID system like the system in Uganda. This paper relies on the two analysis strategies presented in the previous section to consider at a high level how digital ID systems might facilitate digital repression under a current democratic government, a future government that starts to backslide, or a newly installed authoritarian government. While each digital ID system may have its own objectives, we use the overall objectives of digital government initiatives for this high level analysis: to make government more coordinated, efficient, resilient, and responsive.

If a digital ID system achieves these objectives, will the risk of digital repression increase or decrease? The analysis strategy presented above considers potential risks (Table 3). Red boxes denote where the highest risk is expected. As digital ID systems make governments more coordinated and efficient, they may also increase the capacity of governments to conduct mass surveillance and targeted persecution. If digital ID systems make governments more responsive by improving voting turnout and allowing citizens to interact more regularly with the government, that could reduce the spread of disinformation or the likelihood of internet shutdowns (green boxes).[18] In other cases, the impact may be neutral (no likely risk of increased digital repression or movement toward less digital repression, orange box).

As digital ID systems expand, it is essential to mitigate the increased risks of surveillance and targeted persecution. These risks vary across countries and with the design of the particular digital ID system and will continue to change over time as a government's commitment to democratic processes and institutions evolves.

18 The responsive/targeted persecution responsive/censorship box are not green, as digital ID can help governments to censor and target individuals as they are less likely to be able to transact anonymously. The balance between responsiveness and lack of anonymity will look different in each context based on many other factors involved (see Figure 2).

TABLE 3: ILLUSTRATIVE table to visualize and discuss the links between a Digital ID investment and digital repression techniques

	DIGITAL REPRESSION TECHNIQUES →				
DIGITAL GOVERNMENT OBJECTIVES: Government can become more… ↓	Surveillance	Disinformation and social manipulation	Internet shutdowns	Targeted Persecution	Censorship
Coordinated	🔴	🟠	🟠	🔴	🟠
Efficient	🔴	🟠	🟠	🔴	🟠
Resilient	🟠	🟠	🟠	🟠	🟠
Responsive	🟠	🟢	🟢	🟠	🟠

Notes: For the sake of this analysis, the completed table uses a simple color scheme to illustrate the potential to increase opportunities for digital repression (red), neutral impact (orange), and potential to mitigate/block opportunities for digital repression (green). When working with a specific initiative, partners are encouraged to fill in each box with context-specific details that illustrate how these dynamics might play out in real time or in a future of democratic backsliding, or if the government changes entirely.

Interoperability

In addition to digital ID, there is a related trend in digital government programs toward interoperable, whole-of-government approaches. These approaches facilitate communication between the technical systems of various government agencies, line ministries, and regional levels (national, district, and village, for example). A whole-of-government approach is facilitated by a comprehensive, **underlying technical architecture** that allows different information management systems to speak to one another, otherwise referred to as interoperability (Higman et al. 2018).

Interoperability promises many benefits, and the lack of interoperability between government systems undermines many development objectives. The lack of interoperable health-data systems during the 2014-2016 Ebola epidemic stifled decision-making and slowed response times (USAID Digital Strategy). Interoperable government infrastructure can take different forms, both in reality and in the literature. All of these approaches incorporate digital ID, as the unique ID number enables individual records to be matched across government databases.[19]

Enterprise architecture and digital stack, described below, are similar but slightly different concepts:

- **Enterprise Architecture:** Refers to a technical system that enables the integration of systems and shared services across government agencies. Having an enterprise architecture in place helps to ensure that each government agency uses the same base technology, making interoperability easier. It refers to the standardization of governing and operating structure to

19 An individual registered as a government salaried employee may have a record in the government human resources database. They may also be below the poverty line, and thus have a record in the social protection registry. These two records can be matched to confirm that they belong to the same individual if they are associated with one ID number. This allows for real time cross-checking between databases which has contributed to the efficient delivery of emergency social protection payments in response to COVID-19. For more on this example, refer to https://thedocs.worldbank.org/en/doc/655201595885830480-0090022020/original/WBG2PxScalingupSocialAssistancePaymentsasPartoftheCovid19PandemicResponse.pdf

ensure that the base technology is used in similar ways as each agency develops and operates systems that meet its specific needs.

- **Digital Stack:** Describes an approach to digital government in which connected key pieces of digital infrastructure link together. A digital stack is more than the sum of its parts because each component is connected. India's digital stack includes a digital ID system, a digital payments system, and a universal payment interface (UPI) to allow banks, companies, and governments to exchange payment information automatically. These three layers are stacked or connected together to ensure seamless alignment and communication between systems (World Bank 2022). India's digital stack is seen as critical to lowering the cost of identification and payments in order to expand financial inclusion (Raman and Chen 2017).

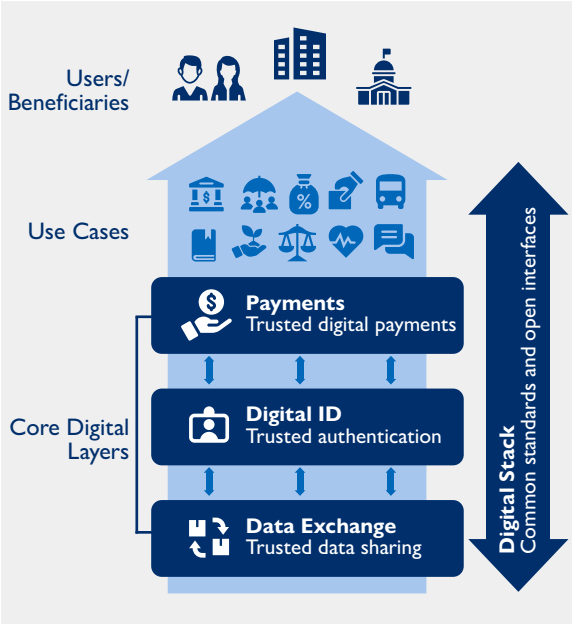


IMAGE 5: The digital stack and its layers
Source: The World Bank, 2022

The potential of interoperable government systems to accelerate development outcomes has been widely discussed, based in large part on the experiences of India and Estonia. India built an interconnected set of systems referred to as the "India Stack" that simplified many processes such as registering individuals for new bank accounts and routing social assistance payments to the intended beneficiaries. This experience has led to digital development investments to help other countries create their own digital stack to build "a more inclusive digital economy from the bottom up" (Carrièrre-Swallow, Haksar, and Patnam 2021).

Estonia has demonstrated the value of enterprise architecture through its X-Road platform, leading development agencies to fund similar approaches in SSA. The government has brought 99 percent of government services online through X-Road and has connected these services to various decentralized identity databases. Citizens have access to any X-Road connected services remotely, from anywhere in the world, through their unique electronic ID number (eID).[20] SSA countries are receiving support from development agencies to work with the Estonia e-Governance Academy (eGA) to adopt the technology, skills, and procedures associated with X-Road (EGA, 2020).[21]

Can the Indian and Estonian models link to digital repression if exported to other countries? The literature does not provide an answer. Thus, we turn to analysis strategies to consider potential links. These models promise to make government more coordinated, efficient, resilient, and responsive.

20 Note that Estonia's ID system is unique in that it is decentralized and thus does not store user data in one central database.

21 EGA is a non-profit think tank and consultancy organization that creates and transfers knowledge in the areas of e-governance, e-democracy, and national cybersecurity. See, for example, "Benin to develop data exchange platform based on Estonian model" https://news.err.ee/882616/benin-to-develop-data-exchange-platform-based-on-estonian-model

Based on the preliminary, high level analysis in Table 4, it can be assumed that interoperability initiatives require mitigation measures that take into account risks across the five tactics. Interoperable systems which make it easier for government agencies to quickly process, share, and analyze data on individuals and organizations can be used for good, perhaps making governments more accountable as these interoperable systems make it easier for people to interact with government agencies (green boxes). However, these systems can also make it easier to surveil, censor, and persecute, by limiting ways for people to interact anonymously when criticizing the government (red boxes). This analysis must be adapted to each country's context and revised frequently to account for the ever-present risks of future democratic backsliding and regime change (Table 4).

TABLE 4: ILLUSTRATIVE table to visualize and discuss the links between interoperable digital government initiatives and digital repression techniques

	DIGITAL REPRESSION TECHNIQUES →				
DIGITAL GOVERNMENT OBJECTIVES: Government can become more… ↓	Surveillance	Disinformation and social manipulation	Internet shutdowns	Targeted Persecution	Censorship
Coordinated	🔴	🟠	🟠	🔴	🔴
Efficient	🔴	🟠	🟠	🔴	🔴
Resilient	🔴	🟠	🟠	🔴	🔴
Responsive	🟢	🟢	🟢	🟢	🟢

Notes: For the sake of this analysis, the completed table uses a simple color scheme to show potential to increase opportunities for digital repression (red), neutral impact (orange), and potential to mitigate/block opportunities for digital repression (green). When working with a specific initiative, partners are encouraged to fill in each box with context-specific details that better illustrate how these dynamics might play out in real time, or in a future of democratic backsliding, or if the government changes entirely.

4.2.2 SECTOR-SPECIFIC DIGITAL DEVELOPMENT OBJECTIVES

Digital development components are increasingly included in projects across different sectors such as health, education, economic growth and trade, and agriculture. These activities often work directly with government line ministries (i.e. the Ministry of Health) to accomplish the same objectives outlined in the previous section (more coordinated, efficient, resilient, and responsive government). In other cases, they may support civil society actors who are working with, and therefore generating data on, vulnerable communities at risk of surveillance and targeting (i.e. a local non-profit organization that provides health services to the LGBTQ community in a country known for persecuting these groups).

The literature describes how sector-specific digital development initiatives may link to digital development. The same analysis strategies can be used in different sectors to prompt a discussion on how sector-focused activities might link to digital repression in real time, or under a future regime that is democratically backsliding or authoritarian. Table 5 provides examples of program objectives for different sectors that are likely to benefit from analysis of their risk of aiding digital

repression now or in the future. To understand these potential connections, refer to Box 8 on public health investments made during COVID-19.

TABLE 5: Illustrating sector-focused digital development investments in terms of their potential impact on digital repression techniques - ILLUSTRATIVE program objectives listed, one for each key sector of interest

	DIGITAL REPRESSION TECHNIQUES →				
PROGRAM OBJECTIVE: Initiative will contribute to improvements in… ↓	Disinformation and social manipulation	Internet shutdowns	Targeting	Surveillance	Censorship
Health system interoperability					
Remote learning (education)					
Financial inclusion (economic growth and trade)					
Access to agricultural information (agriculture and food security)					

Notes: The objectives listed on the left are illustrative rather than exhaustive.

BOX 8: COVID-19 enables government surveillance and infringement on rights in the name of public health

The COVID-19 pandemic has made it harder to ignore the intersection between digital repression, economic development, and inclusion. Efforts to stem the spread of the virus, such as contact tracing, have been viewed as aiding in mass surveillance and tracking for political purposes, demonstrating how digital investments made on behalf of public health can potentially provide additional tools and justification for digital repression.

There are documented instances of digital repression ascribed to COVID-19 across the five types of digital repression. Between March 2020 (the beginning of the pandemic) and June 2021, the V-Dem Institute tracked violations of democratic standards related to COVID-19 measures in 144 countries (although the rate of violations has declined over the course of the pandemic). These violations include limiting legislative oversight, restricting media freedom, and engaging in abusive enforcement of restrictions (V-Dem Institute 2021).

Examples below show that digital repression was less common than feared in Nigeria, and improved over time in Tanzania, demonstrating ways in which democratic institutions (data protection authorities and elections, respectively) can protect against long-term overreach. These examples include:

Censorship: In Uganda, the Electoral Commission banned in-person political campaigning in June 2020, nominally in order to prevent the spread of COVID-19. However, the restrictions provided a clear advantage to the ruling party, which has unrestricted access to media, while the opposition was left with few ways to communicate with the electorate (Freedom House 2021). Militarized enforcement of restrictions was reported early on in the pandemic in countries including Malawi, Kenya, Nigeria, Zimbabwe, and Rwanda (Ilori 2020).

BOX 8 (CONTINUED): COVID-19 enables government surveillance and infringement on rights in the name of public health

Disinformation: Tanzania's former President John Magufuli launched one of the continent's most aggressive COVID-19 denialism campaigns in early 2020, claiming that prayer was the best remedy for the virus. He was replaced by President Samia Suluhu Hassan who has taken the opposite approach, embracing the global scientific consensus and publicly receiving her vaccine. However, the damage from the original government-led disinformation campaign combined with rampant misinformation from a diverse range of other sources has caused lasting damage to public trust in public health information, challenging the country's current efforts to increase vaccine uptake (Makoye 2021).

Targeting of individuals: In Kenya, the government arrested four individuals in March 2020 under section 23 of the Computer Misuse and Cyber Crime Act for publishing information that countered the government's claims regarding the virus (CIPESA 2021).

Surveillance: Despite concerns expressed at the beginning of the pandemic that COVID-19 would be used to justify mass surveillance, there are few reported occurrences of this happening in SSA. Nigeria raised concerns in April 2020 with its plans to monitor cellphone data, however research found that this initiative complied with data protection guidelines. Data protection authorities (DPAs, see Section 5.3.3) across SSA have played a role in ensuring compliance with DPAs in many countries (Ilori 2020).

Internet shutdowns: Social distancing measures put in place to mitigate the spread of COVID-19 have made mobile and internet access more vital than ever. The internet provides access to important information about the disease, while essential services for health and education are increasingly provided remotely and online (UNESCO 2020). Research among marginalized and hard-to-reach populations in Zimbabwe found that these communities rarely received messaging on COVID-19 disease prevention, identification, and treatment (Mhlanga et al. 2021). When governments intentionally shut down the internet across all or part of their country, those marginalized from existing services are less likely to be able to obtain access to essential needs and services, resulting in "unprecedented consequences on the lives of the most vulnerable" (AccessNow 2020).

5. Risk Mitigation: What is already happening?

How can identified risks be mitigated? Development actors, civil society, government, and the private sector all have a role to play in mitigating digital repression so the benefits of digital development can be realized without enabling or being undermined by digital repression. While the literature reviewed suggests that there is not yet a sufficiently coordinated effort underway to prevent digital repression in SSA, a diverse range of examples of mitigation efforts are driven by different stakeholder groups. Many of the mitigation efforts target a specific digital repression tactic, while others work to protect against overall digital repression. The list below highlights examples of risk mitigation that target the intersection of digital development and digital repression. (This is not an exhaustive list.)

5.1 DEVELOPMENT ACTORS

International development actors—including multilateral donors, foundations, and implementers—are employing a variety of strategies in the face of digital repression. Development actors are looking at digital security within their specific sectors, while those focused on democracy, rights, and governance are working to increase the capacity of government and civil society. These efforts will be more effective when the two streams are better aligned (Section 6).

5.1.1 PRINCIPLES

Development organizations have led efforts to design principles related to specific topics in digital development. Principles stem from a recognition by the international development community that digital technologies bring risks along with opportunities. They are intended to provide flexible and non-binding guidance for practitioners interested in ensuring that projects are successful and inclusive. The Principles for Digital Development, endorsed by more than 100 organizations working in international development, aim to integrate best practices into technology-enabled programs. The nine principles include *Address Privacy and Security* and *Understand the Existing Ecosystem.*

The Principles on Identification for Sustainable Development were published in 2017 and revised in 2021. They are managed by the World Bank and endorsed by 30 organizations. These principles are focused on government ID systems and aim to support (as the first principle) universal access for individuals, free from discrimination. In addition to the focus on inclusion, relevant principles include *Create a responsive and interoperable platform, Protect privacy and agency through system design,* and *Establish a trusted—unique, secure, and accurate— identity.*

One sector-focused example is the Health Data Governance Principles. In recognition that the increase of availability in timely health data offers huge benefits as it also presents significant risk to marginalized

communities, partners including Transform Health, PATH, RECAINSA, AeHIN, Governing Health Futures 2030, and Young Experts: Tech 4 Health are undertaking a consultative process to develop a set of Health Data Governance Principles. To date, participants have advocated for interoperable data standards and cross-border data- sharing protocols.

5.1.2 INTERNAL DATA GOVERNANCE

Development actors, like governments, collect data on vulnerable populations and this data can present risks. Data contained in development databases can be used for surveillance and targeting if not properly secured. Donors and implementers have made strides in this area in recent years. Considerations for Using Data Responsibly at USAID offers guidance on how USAID and partner organizations can implement responsible data practices. The document contains resources on data privacy, open data, and data quality. It aims to raise awareness on data concerns and to promote conversations on data privacy within the international community.

5.1.3 SUPPORT FOR CIVIL SOCIETY AND MEDIA

Several USAID programs have integrated training for civil society and media professionals into conflict stabilization programs. USAID's flagship internet freedom program, Greater Internet Freedom (GIF) [internal USAID link] works with civil society, human rights defenders, and independent media to enhance digital security and increase citizen engagement in Internet governance. The Office of Transition Initiatives (OTI) Ethiopia Program started working with local university students in 2019 on how to monitor and identify mis- and disinformation on social media, as well as how to create new content for social media that is constructive to political dialogue. The OTI Sudan Program is doing similar work with independent media.

USAID's Georgia Information Integrity Program addresses ways to counter the spread of disinformation through partnerships with media organizations, universities, digital researchers, and civil society. The program aims to identify, monitor, and prevent the spread of disinformation online.

5.1.4 RESEARCH AND TRANSPARENCY INITIATIVES

Global actors are supporting research to better understand the dynamics of digital repression, calling attention to gaps, challenges, and uses of various tactics in SSA and elsewhere. The Disinformation Tracker was launched in 2020 by partners including Global Partners Digital (GPD), ARTICLE 19, CIPESA, PROTEGE QV and the Centre for Human Rights of the University of Pretoria. The website provides an interactive map to track disinformation laws and policies across SSA and offers trends, analysis, and a framework to assess the status of state responses to disinformation across the region. USAID has funded or published several resources, including the Disinformation Primer, the Digitized Autocracy Literature Review, and the Cybersecurity Primer: How to Build Cybersecurity into USAID Programming.

The Africa Infodemic Response Alliance (AIRA), supported by the World Health Organization (WHO), is an example of the convening power of the international community. AIRA is a network for sharing safe and proven facts on health to counter dangerous health misinformation. The Alliance addresses the spread of misinformation in digital environments and brings together fact-checkers, media organizations, big data, AI, and civil society leaders. AIRA applies four pillars to their approach: identify, simplify, amplify, and quantify.

5.1.5 GOVERNMENT CAPACITY-BUILDING

The international development community engages regularly with governments to build capacity around digital tools and data governance. Organizations such as DIAL and Smart Africa help governments develop digital strategies, while the World Bank and others work directly on the development and implementation of data protection laws across SSA, and USAID works with partner governments to embed technical assistance. USAID worked with the West African Health Organization to embed a team of informatics experts to strengthen the region's health information systems. Through its ProICT activity, USAID also provides technical assistance and capacity-building to help developing country governments establish ICT policy and regulatory frameworks. While these efforts do not always focus on preventing digital repression, there is an opportunity to integrate more content on digital democracy, rights, and governance in this work, as will be discussed in Section 6.

5.2 CIVIL SOCIETY AND MEDIA

Civil society and media actors in SSA play a critical role in calling attention to government use of digital repression, opening civic space online when it is closed by the government, protecting individuals who may be targeted for online speech, and litigating government digital repression in national and international courts. Civil society and media play a critical role in fighting digital repression in all countries—even if these efforts are often slow and challenging.

5.2.1 MULTI-STAKEHOLDER AND CROSS-COUNTRY ADVOCACY CAMPAIGNS

In recent years, civil society has used social media platforms, especially Twitter, to mobilize against digital repression, using digital activism to overcome digital repression. The campaigns are organized through hashtags and often attract international attention which increases pressure on governments. The #KeepItOn coalition against internet shutdowns includes 258 organizations from 106 countries, including companies such as Twitter. As one indicator of the influence of this campaign, in May 2021, the G7 Foreign and Development Ministers' Meeting issued a communiqué that condemns "actions by states to intentionally disrupt their own populations' access to, or dissemination of, information, knowledge, and data online (Access Now 2021)." Similar efforts include #BringBackOurInternet which advocated for an end to long-running network disruption in Cameroon, and #InternetFreedomAfrica that raises awareness on internet freedom issues in Africa.

When the government of Benin introduced a tax on social media, the offline and online #TaxePasMesMo advocacy campaign successfully prompted the country's leaders to suspend its implementation (CIPESA 2019). On the other hand, the #NoToSocialMediaTax in Uganda has yet to result in removal of the tax, despite attracting international attention (Freedom House 2021).

5.2.2 FACT-CHECKING TO COUNTER DISINFORMATION

A number of fact-checking organizations operating across Africa such as Africa Check, Pesa Check, Media Monitoring Africa, and iLab work together and with social media platforms to monitor and debunk some of the most egregious and widespread disinformation online (DFR Lab 2021). These organizations find it more difficult to work with end-to-end encryption platforms known for their digital security, such as WhatsApp and Telegram. The high level of security makes it harder for governments to surveil and censor content, but also has the unintended consequence of making it

more difficult to determine the source of fake stories that circulate on these platforms, just as they circulate on non-encrypted social media platforms (Africa Center for Strategic Studies 2021).

Fact-checkers track down and contact people making false claims to ask them about their sources and proof; check with experts in the field to add nuance and context in disproving each claim; and write and disseminate briefs with facts and evidence to systematically disprove false information. This work takes time, and by the time fact-checkers are able to establish and disseminate the truth, much damage has already been done. The work of fact-checkers must be complemented by efforts to stop the dissemination and consumption of disinformation in the first place (Africa Center for Strategic Studies 2021).

5.2.3 KNOWLEDGE AND TRAINING ON DIGITAL RIGHTS FOR CONSUMERS, ACTIVISTS, COMPANIES, AND SOCIAL SERVICE ORGANIZATIONS

Knowledge and training on digital rights applies broadly across the private sector and civil society. There are a number of efforts to help activists communicate securely and without interruption by circumventing government surveillance and censorship. Access Now Digital Security Helpline provides 24/7 assistance free of charge in nine languages. The Electronic Frontier Foundation produced a *Surveillance Self-Defense* guide with tips on how to circumvent online spying, providing analysis of secure applications and a list of common security scenarios.

The private sector is increasingly aware that digital risks can affect the ability of customers to participate in the digital economy. A growing body of work on consumer risks in areas including digital financial services and e-commerce addresses the overarching goal of expanding digital rights.

5.2.4 LITIGATION: DOMESTIC COURTS

Civil society can sue a government for legal violations as a way of calling attention to digital repression, taking advantage of the legal system as a check on government overreach. There are examples of litigation across the five tactics of digital repressions. Litigation against internet shutdowns has been undertaken in Cameroon, Chad, The Gambia, Togo, Uganda, and Zimbabwe (This is not an exhaustive list). When the Government of Zimbabwe imposed social media blocking and network shutdowns in the face of protests in January 2019, the Media Institute of Southern Africa (MISA) and the Zimbabwe Lawyers for Human Rights (ZLHR) sued the government. Within a few days, the High Court declared the shutdown illegal, stating that the Minister of State for National Security lacked the authority to issue directives under the Interception of Communications Act, which he had used to order the shutdown (CIPESA 2019 and Freedom House 2019).[22]

Civil society-driven court cases are not always successful. Still, they help to document and bring attention to repressive tactics. In 2021, Unwanted Witness Uganda brought a case against the government and service providers for social media blocks during the 2016 election period to the Constitutional Court. The case was dismissed, holding that the restrictions were permissible under Article 43 of the Uganda constitution, which permits the limitation of constitutionally-protected fundamental rights and freedoms (Freedom House 2021).

22 This ruling was not made on constitutional grounds, and thus left open the possibility for future government shutdowns.

5.2.5 LITIGATION: REGIONAL AND INTERNATIONAL COURTS

When domestic courts are weak, or the domestic legal framework is not sufficient to protect against digital repression, civil society is finding some success in litigating violations in regional or international courts. In 2020, Amnesty International sued the Republic of Togo in the Economic Community of West African States (ECOWAS) Court, challenging the government's decision to shut down the internet during protests in September 2017. The Court declared that internet shutdowns are unlawful under Article 9 of the African Charter on Human and Peoples' Rights as the internet is an essential element in human rights enjoyment, in particular, the right to freedom of expression and the right to access information (Columbia University 2020).

In Uganda, the East Africa Law Society (EALS) challenged the January 2021 internet shutdown in a petition filed at the East African Court of Justice (EACJ), seeking a declaration that the shutdown was illegal and asking for compensation for users. The case, filed in March 2021, is ongoing as of this writing (Freedom House 2021).

A recent example of international litigation (outside of SSA) is a multi-country effort to sue Meta, Facebook's parent company, for $150 billion USD for the platform's role in inciting violence against the Rohingya in Myanmar. The suit was filed in a California court on behalf of an estimated 10,000 Rohingya refugees who have settled in the United States since 2010, and relies heavily on a UN fact-finding mission that identified hate speech and propaganda—spread on Facebook and promoted through the company's algorithms—as a key contributing factor to human rights violations against the Rohingya. Facebook admitted in 2018 that it had not done enough to prevent this violence (Ingram and Darrach 2021).

5.3 GOVERNMENT

Governments can set up mechanisms, laws, and policies to protect against current and future digital repression. These range across the five tactics of digital repression and include strengthening checks on government and strengthening data protection laws and implementation bodies.

5.3.1 ESTABLISHING INDEPENDENT MECHANISMS/CHECKS

To prevent repression in the face of democratic backsliding, some governments are creating independent mechanisms that hold government bodies accountable by requiring oversight and approval for policy decisions such as internet shutdowns or censorship.

Efforts to accomplish this are ongoing in Uganda, where many of the tactics described in this paper are implemented by the Uganda Communications Commission (UCC). The UCC is not entirely independent of the executive branch, as the ICT minister sits in the President's office and has the authority to approve the UCC's budget and appoint members of its board. In January 2021, the UCC issued a call for comments on the Uganda Communications Tribunal (Practice and Procedure) Regulations 2020, which mandated more accountability to the public by creating a tribunal with jurisdiction over all matters relating to communications services arising from decisions made by the UCC and the ICT minister. While it remains to be seen whether the Tribunal will be staffed in such a way that it is truly independent, this is a good example of the type of check that democratic governments can implement to protect against present and future repression (Freedom House 2021).

5.3.2 DATA PROTECTION FRAMEWORKS

Africa's legal environment for ensuring data protection and privacy is described as "underdeveloped and disparate in spite of some dynamic and progressive frameworks and laws" (Africa Digital Rights Hub 2019, 2). While data protection law across the continent is nascent, foundations are in place. Most African countries recognize the right to privacy as a fundamental right enshrined in the constitution. And there are several relevant regulations at the continental and regional levels, including the African Union Convention on Cyber Security and Personal Data Protection (2014), also known as the Malabo Convention[23]; the Southern African Development Community (SADC) Model Law on Data Protection (2010); ECOWAS' Supplementary Act A/SA.1/01/10 on Personal Data Protection (2010); and the East African Community (EAC) Framework for Cyberlaws (2008). As of August 2020, 29 SSA countries had some data protection legislation in place, although not all of this legislation is fully implemented as of this writing.[24]

Many country frameworks are modeled after Europe's General Data Protection (GDPR) framework, an omnibus law that guides the collection, processing, and sharing of personal data for both the public and private sectors (International Bar Association 2021, 14). African governments are under pressure to harmonize their data protection frameworks with GDPR, especially from businesses that want to transact with the EU and therefore must comply with EU privacy standards (ID4Africa 2019). The United States has two data protection certifications which can serve as models for SSA: the APEC Cross-Border Privacy Rules (CBBR) and Privacy Recognition for Processors (PRP) systems.[25]

Data protection law in SSA may be nascent, but there are examples of it countering government digital repression. In October 2021, the High Court in Kenya declared the government's rollout of the new national digital ID, *Huduma Namba*, unconstitutional on the grounds that it did not comply with the Data Protection Act (2019) as no data protection safeguards were implemented by the Ministry of Interior and Coordination of the National Government. Although the Data Protection Act came into force after the *Huduma Namba* initiative was planned, the Judge declared that the Act should have been enacted retroactively. Based on this ruling, the ministry was ordered to conduct an impact assessment on data already collected on 36 million Kenyans before moving forward. Echoing the importance of civil society, the case was brought to court by the Katiba Institute, a nonprofit established in 2011 to defend and ensure implementation of the Constitution of Kenya (Wasuna and Wangui 2021).

5.3.3 DATA PROTECTION AUTHORITIES (DPAS)

Many governments are mandated to appoint a data protection authority (DPA) to implement and enforce data protection legislation. As of July 2020, 11 African countries had DPAs, while government agencies in 18 SSA countries are members of the Network of African Data Protection Authorities (RAPDP, acronym for the French translation).[26] Most are poorly resourced and lack the ability to attract the high caliber staff necessary for these agencies to enforce data protection regulations

23 The Malabo Convention, adopted in 2014, was modeled on the EU Data Privacy Directive 95/46/EC, which has since been replaced by GDPR. The Malabo Convention is out of date and incomplete (only 15 countries have signed), although it remains an important influence in Africa and was still open for signature as of 2019 (ID4Africa 2019, International Bar Association 2021).

24 Number based on the Data Protection Africa portal, last updated 3 August 2020. https://dataprotection.africa/

25 CBPR certifications are being considered for use outside of APEC countries.

26 Some members are not explicitly DPAs although they have some data protection responsibility, including South Africa's Information Regulator and the Uganda National Information Technology Agency. For the full list, visit www.rapdp.org

(International Bar Association 2021, 14). DPAs play a role in educating other parts of the government—including the authorities mandated with implementing digital ID—on data risks and privacy impacts of new technologies such as biometrics. They also handle privacy complaints from the public. In 2019, DPAs in Africa reported increases in privacy complaints of 20 to 30 percent in just a few years, signaling an increased awareness of data protection and DPAs in these countries (ID4Africa 2019).

5.4 PRIVATE SECTOR

The private sector is comprised of a wide range of actors, including global social media companies, telecommunications companies, and Africa-based technology startups. Social media companies that control platforms that spread disinformation are often the target of censors, and have a complex role to play. This paper does not detail the ongoing debate on platform regulation or specific practices of social media companies to control disinformation. This section details practical steps that technology companies are taking to mitigate digital repression globally and in SSA.

5.4.1 TRANSPARENCY REPORTING

Corporate transparency reports can be produced by any company operating online or processing digital data, including social media companies, internet service providers, online news journals, and MNOs. These reports take different forms, but in general they disclose government requests for information on groups or individuals, illuminating the scope and scale of online surveillance, internet shutdowns, and censorship. They provide information on networks that have been identified as spreading disinformation, and they can provide insight into a company's policies and safeguards against government abuses (Access Now 2021).

Africa (along with Latin America) lags behind other regions in producing corporate transparency reports. As of 2021, the only African company that had produced such a report in recent years was Liquid Telecom, based in Kenya (Access Now 2021).[27] The international community and investors can exert pressure on companies to produce transparency reports in order to deepen understanding and mitigation of digital repression.

5.4.2 INNOVATIVE SOLUTIONS

The private sector plays a critical role in providing new tools for use by individuals in continuing to communicate in the face of digital repression. As governments start to block some forms of communication (i.e. Facebook and Twitter), companies can quickly provide such new tools. Encrypted messaging apps including Signal and WhatsApp help to avoid censorship, and VPNs can be used to stay online despite shutdowns.[28]

Digital ID is another area where the private sector is providing new solutions to mitigate risks of surveillance and targeting. Distributed identity technology (also referred to as self-sovereign identity), can securely provide the benefits of ID services without simultaneously providing governments unbridled access to user data. This technology is used for the EU COVID certificate. Personal data

27 As reported by Access Now, although the authors were unable to find this report on Liquid Telecom's website.

28 The use of both Signal and Telegram spiked in Ukraine immediately after the Russian invasion. However, Telegram is not fully encrypted and does not offer an option for disappearing messages and thus may not meet the full range of security needs. For a detailed analysis of the benefits and risk of various messaging apps for people in both Ukraine and Russia as of March 2022, refer to: https://www.eff.org/deeplinks/2022/03/telegram-harm-reduction-users-russia-and-ukraine

is only stored on each individual's phone, and that person decides which information to share and who to share it with. An individual can show their employer that they have received three vaccinations and can opt to show only a negative test result to a local restaurant. This type of technology, yet to be adopted at scale, is becoming more accessible. The EU COVID certificate was developed and launched in just a few months (Schubert 2021).

5.4.3 ADVOCACY AND ENGAGEMENT

There are severe economic costs to digital repression. Internet shutdowns cost countries an estimated $2.4 billion per year (Allen, Hass, and Jones 2016), while censorship and surveillance create a culture of fear that limits economic activity online. Disinformation can target companies as well as individuals and civil society. The private sector plays a key role in engaging with the government to advocate against the use of digital repression.

A group of 51 CEOs from the United States sent an open letter to the U.S. Congress asking for more comprehensive data protection, even offering a framework for what such a law might look like (Fingas 2019). In Pakistan, companies supported think tanks, consulting firms, and NGOs to build an evidence base on the economic costs of internet disruptions, and have even contributed to litigation against shutdowns (Sullivan 2020).

6. Recommendations for USAID and Development Partners

USAID is pushing forward with the promotion of safe, secure, and effective expansion of digital ecosystems to support positive development outcomes. This commitment is signaled by the adoption of the Digital Strategy, the publication of the Digital Ecosystem Assessment Framework (DECA), and the recent creation of a new Chief Digital Development Officer position. Digital development is not only a priority for USAID, but across the U.S. Government, as signaled by whole-of-government initiatives such as the Digital Connectivity and Cybersecurity Partnership (DCCP). USAID implementing partners are investing in digital development, as signaled by interest in events such as the Global Digital Development Forum.[29]

How can USAID and its partners use this momentum to ensure that digital development efforts mitigate the risks associated with digital repression? The mitigation strategies listed in Section 5 highlight ways that various stakeholders are currently attempting to prevent the misuse of technology. However, as the trends described in Section 2 illustrate, these efforts are insufficient in the face of worsening digital repression and democratic backsliding in recent years. USAID and development partners alone cannot protect against digital repression, but they can do more to ensure that technology investments paid for with development funds are not used to advance digital repression.

Many of the recommendations below focus on **shifting from a defensive approach to an offensive approach to preventing digital repression.** Digital development practitioners are generally aware of standard best practices, such as the need for data protection and privacy measures. However, these defensive practices are insufficient. If an authoritarian government comes to power in a previously democratic country and obtains access to the country's existing digital government systems, they are unlikely to respect existing data protections and privacy practices. Recognizing this, how can initiatives take a more offensive approach?

6.1 SHORT-TERM ACTIONS OR QUICK-WINS

Use existing resources. A good first step is to ensure broad awareness of existing resources. These include the Digital Principles, the Cybersecurity Primer, the Disinformation Primer, Using Data Responsibly at USAID, and the Gender Digital Divide Primer, among others. While the teams that developed these resources are working to disseminate them widely, their efforts can be amplified. These resources can inform a conversation on links to digital repression tactics not yet covered.

29 The May 2020 Global Digital Development Forum (GDDF) was co-organized by USAID, Chemonics, Deloitte, and TechChange had over 2,600 participants.

Provide questions for USAID staff and implementers to ask in order to fully integrate digital repression risks into Digital Ecosystem Assessments. USAID's Digital Ecosystem Framework (Figure 1) encourages USAID and its partners to recognize the larger socioeconomic and political environment in which digital investments and activities operate. It is designed to provide a comprehensive overview and shared understanding of the elements that influence a country's digital ecosystem and encourages consideration of digital repression and digital rights. The analysis strategies put forward in this paper can be refined and expanded to prepare specific guidance that encourages consideration of all five digital repression risks.

Integrate talking points on digital repression risks into ongoing conversations with governments and development partners. USAID Operating Units (OUs), leadership, and interagency partners are engaging with key actors in digital development and digital government. This includes Mission staff working with government counterparts in host countries and Washington-based staff engaging with global partners such as DIAL, Smart Africa, Estonia e-Governance Academy, the World Health Organization, and other UN agencies and bilateral donors. There are many ways to integrate a higher understanding of digital repression into these conversations: (1) developing and sharing talking points with Mission staff and USAID leadership; (2) integrating talking points into workshops and conversations with Mission-based Digital Development Advisors; (3) integrating talking points into workshops and conversations with Washington-based staff managing these partnerships; (4) hosting conversations on digital repression with external partners.

Integrate consideration of present and future digital repression risks into relevant requests for proposals (RFPs). Digital technology is increasingly integrated into sector-specific programming. USAID Pillar Bureaus (Health, Education, Resilience and Food Security, Economic and Market Development, and Humanitarian Assistance) can encourage implementing partners to incorporate language on digital repression into RFPs.

6.2 MIDTERM INVESTMENT OPPORTUNITIES

Identify opportunities in sector-specific initiatives to provide technical assistance or financial support for civil society and media organizations. As demonstrated in this analysis, capacity among a wide variety of democratic institutions is needed to mitigate risks of digital repression. If a digital health activity focuses only on the health sector, it may overlook opportunities to work with the court system to ensure that the courts understand how to litigate the misuse of personal health data. Using the analysis tools provided in this report and IDEA's 28 indicators of a democracy, a *guidance note* can encourage sector-focused colleagues to look at each indicator in terms of potential areas for strengthening in order to mitigate near and long-term risks.

Engage with social media companies on practical steps to improve access and understanding of verified content. Facebook, Twitter, and other social media platforms drive the ways people access information and actively promote disinformation and fake news due to their ability to shock and gain attention. These companies hold the power to change their algorithms to slow the spread of dis-, mis-, and malinformation. Development actors can work with companies to increase staff diversity throughout SSA (not only in regional hubs such as Nairobi and Johannesburg) as well as content in local languages, which is fundamental to the fight against disinformation. In Uganda, there are 40 languages and 56 indigenous dialects. Yet, Google Uganda is available in only five of those

languages. News sites owned by Vision Group, partially owned by the government, are available in four of the languages, and many privately owned online newspapers are only available in English (Freedom House 2021, DFR Lab 2021).

Strengthen official, continuously updated, independent, and secure statistical databases. Most governments have their own statistics division set up to collect and process census and health data. If these are inaccurate or out of date, external actors may publish and disseminate incorrect information. If data is inaccessible due to bureaucratic red tape or other reasons, journalists and researchers will turn to less reliable secondary sources. Statistical databases—secured and managed by independent bodies—can hinder the ability of a new authoritarian government or a democratic government that is actively backsliding to manipulate historic information for their own benefit (Fayoyin and Ngwainmbi 2015). *While these efforts may present their own risks, governments are still investing in them. USAID can play a role in ensuring that they are safe, secure, and trusted.* Consult the World Bank regarding their support for the improvement of civil registration systems under the ID4D initiative.

Encourage development, government, and civil society partners to complement digital approaches with non-digital approaches where relevant. Consider models of community development that disseminate information through analogue methods such as community radio, and indigenous structures including traditional leaders, religious heads, social workers, and healers (Mhlanga et al. 2021). These structures were instrumental during COVID-19. Countries that had the most success with remote education during the pandemic implemented context-appropriate remote learning strategies that leveraged multiple modalities, including online learning, radio and TV, mobile phones, and printed take-home materials (World Bank 2021). This is relevant across many types of programs, including health, education, and democracy and governance.

Support research on the disproportionate impact of digital repression on women and other marginalized groups. Gaining a more nuanced understanding of how different groups experience the tactics of digital repression can help to prevent and mitigate impact on those already facing systematic inequality. This research can be used in conversation with gender experts across sectors as to how considerations of digital repression can support their work.

6.3 OVERALL APPROACHES, OR LONG-TERM SHIFTS

Emphasize the urgency of adapting a future-lens to the planning of digital development activities. As the example of Afghanistan demonstrates, implementing digital development activities for one government without considering the possibility of future regime change can lead to disastrous consequences. Widespread dissemination of the three questions provided in Section 4 can encourage a long-term view and allow for contingency planning.

Consult with democracy and governance experts, local civil society activists, and local legal practitioners early in the planning of a digital development initiative. USAID's Disinformation Primer recommends working directly with partner countries to implement whole-of-government approaches that bring in private and civil society sectors and media. This can be expanded to focus on all five digital repression tactics and include development actors focused on sectors other than democracy and governance. In some countries, this may mean not working directly with the government, but still bringing together different voices to create a coherent approach.

Ask critical questions of technology service providers, especially if it is proprietary technology from the United States or other global companies. US-based technology is not inherently more democratic than technology from other countries. The vast majority of companies put their own profit interests before other objectives. Private sector partnerships, while critical to digital development, must be approached with caution, understanding that a company's objectives will never be entirely aligned with USAID's development objectives. Open-source technologies can be more flexible than proprietary technologies, however, these technologies are not free and ongoing maintenance and upgrade costs and human resources needs must be taken into account. For more on this, check on the Digital Public Goods Alliance, the How-to: Avoid Vendor Lock-In section of USAID's Digital ID Guide, and the FinTech Partnerships Playbook.

Encourage Mission-based staff to work with government counterparts to view data protection as an opportunity rather than as a costly burden. Data protection is often viewed first as a cost, leading to underfunded or non-existent DPAs and diminishing the capacity of government, business, and legal professionals to increase compliance. Yet, improving data protection in SSA is likely to deliver a large financial upside for countries. Robust and harmonized data protection is critical to implementing the African Continental Free Trade Area (AfCFTA) and to promoting trade with foreign countries, including the United States and Europe. Multinational companies and local African companies looking to expand to new markets have to create dozens of services to comply with the laws in each country (Nwafor 2020). Focusing on the economic benefits of data protection law and harmonization will encourage investment in the data protection laws and agencies needed to protect against misuse of personal data, surveillance, and targeting.

7. Concluding Remarks

Digital ecosystems can drive a wide range of benefits for government, business, and society. It is necessary to assess digital development not only in terms of access, but also in terms of quality and security in order to realize these benefits. Higher internet speeds and numbers of mobile phone subscriptions measure access, but these indicators can be undermined by digital repression. Censorship and target persecution can keep women and other marginalized groups from using their mobile phones if they do not feel safe, while high-speed internet can still be shut down, cutting entire countries off from online economic activity, news, and health information, impeding online transactions and access to information.

Recent events have magnified the risks associated with digital repression. COVID-19 responses demonstrated how governments can disregard digital rights in the name of public health, while the Russian invasion of Ukraine demonstrates the immense power of disinformation campaigns to skew reality and justify real world violence and destruction. The global trend of democratic backsliding increases these risks worldwide.

These complex issues cannot be ignored. Even without documented evidence of the precise risks in all cases, development practitioners can still ask questions that lead to critical discussion about potential links between digital repression and digital development initiatives. Asking how risks might change in the future and how project objectives might link to digital repression are good ways to open a conversation.

A concerted effort is required to leverage advancements in technology to drive sustainable development. In addition to asking critical questions, effective mitigation requires aligning and strengthening current efforts. Development actors, private sector companies, civil society organizations, and governments are increasingly aware of digital risks. Integrating a thorough understanding of digital repression and digital rights into ongoing efforts will amplify their impact. Digital technology can drive a more equal future, but it will take intentional efforts to shift the power of these tools to those who need them the most.

REFERENCES

AccessNow. 2020. "Civil society to WHO: let's end government-ordered internet shutdowns." https://www.accessnow.org/civil-society-to-who-lets-end-government-ordered-internet-shutdowns/.

Access Now. 2021. "#KeepItOn update: who is shutting down the internet in 2021?" https://www.accessnow.org/who-is-shutting-down-the-internet-in-2021/#fight-back-with-KeepItOn.

Access Now. 2021. "Transparency Reporting Index." https://www.accessnow.org/transparency-reporting-index/.

Africa Center for Strategic Studies. 2021. "Africa Check: Sorting Facts from Fakes – Africa Center for Strategic Studies." Africa Center for Strategic Studies. https://africacenter.org/publication/africa-check-sorting-facts-from-fakes/.

Africa Center for Strategic Studies. 2021. "Domestic Disinformation on the Rise in Africa – Africa Center." https://africacenter.org/spotlight/domestic-disinformation-on-the-rise-in-africa/.

Africa Digital Rights Hub. 2019. "Data Protection Code of Practice for Digital Identity Schemes in Africa." https://africadigitalrightshub.org/wp-content/uploads/2021/06/Data-Protection-Code-of-PracticeEnglish-Soft-Copy.pdf.

Allen, John R., Ryan Hass, and Bruce Jones. 2016. "Internet shutdowns cost countries $2.4 billion last year." Brookings Institution. https://www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/.

Amnesty International. 2021. "Uganda: Authorities must lift social media block amid crackdown ahead of election." https://www.amnesty.org/en/latest/news/2021/01/uganda-authorities-must-lift-social-media-block-amid-crackdown-ahead-of-election/.

APC. 2021. "Uganda 2021 general elections: The internet shutdown and its ripple effects." Association for Progressive Communications (APC). https://www.apc.org/en/news/uganda-2021-general-elections-internet-shutdown-and-its-ripple-effects.

Athumani, Halima. 2021. "Ugandan Writers, Poets Decry Re-Arrest of Award-Winning Author." *VOA*, December 30, 2021. https://www.voanews.com/a/ugandan-writers-poets-decry-re-arrest-of-award-winning-author/6375665.html.

BBC. 2007. "Zimbabwe: Phone, internet firms installing surveillance gear." August 30, 2007. https://www.proquest.com/wire-feeds/zimbabwe-phone-internet-firms-installing/docview/452260367/se-2?accountid=11752.

Becker, Celia. 2021. "Taxing the digital economy in sub-Saharan Africa." International Bar Association. https://www.ibanet.org/Taxing-the-digital-economy-sub-Saharan-Africa.

Bradshaw, Samantha, and Philip Howard. 2019. "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation." University of Oxford. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf.

Carrièrre-Swallow, Yan, Vikram Haksar, and Manasa Patnam. 2021. "The India Stack is Revolutionizing Access to Finance - IMF F&D." IMF. https://www.imf.org/external/pubs/ft/fandd/2021/07/india-stack-financial-access-and-digital-inclusion.htm.

Chutel, Lynsey. 2018. "China is exporting facial recognition software to Africa, expanding its vast database." *Quartz Africa*, May 25, 2018. https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/.

CIPESA. 2019. "Digital Rights in Africa: Challenges and Policy Options copy." https://cipesa.org/?wpfb_dl=287.

CIPESA. 2019. "State of Internet Freedom in Africa: Mapping Trends in Government Internet Controls, 1999-2019." http://www.ictworks.org/wp-content/uploads/2022/01/Internet-Freedom-in-Africa.pdf.

CIPESA. 2021. "How the Covid-19 Fight Has Hurt Digital Rights in East Africa copy." https://cipesa.org/?wpfb_dl=427.

CIPESA. 2021. "How African governments are undermining the use of encryption." *Collaboration on International ICT Policy for East and Southern Africa (CIPESA)*, October 26, 2021. https://ifex.org/how-african-governments-are-undermining-the-use-of-encryption/.

Columbia University. 2020. "Amnesty International Togo and Ors v. The Togolese Republic." Global Freedom of Expression. https://globalfreedomofexpression.columbia.edu/cases/amnesty-international-togo-and-ors-v-the-togolese-republic/.

Comparitech. 2021. "Internet Censorship 2021: A Global Map of Internet Restrictions." https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/.

Crumpler, William. 2021. "The Human Rights Risks and Opportunities in Blockchain." CSIS. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/211214_Crumpler_HumanRights_Blockchain.pdf?arkH_fAUfQAlZExHYUfrq6XWks9.SPwN.

Deloitte. 2016. "The economic impact of disruptions to Internet connectivity: A report for Facebook." Deloitte. https://www2.deloitte.com/global/en/pages/technology-media-and-telecommunications/articles/the-economic-impact-of-disruptions-to-internet-connectivity-report-for-facebook.html.

DFR Lab. 2021. "Eritrean report uses fact-checking tropes to dismiss evidence as "disinformation."" Medium. https://medium.com/dfrlab/eritrean-report-uses-fact-checking-tropes-to-dismiss-evidence-as-disinformation-385718327481.

Diamond, Larry. 2010. "Liberation Technology." *Journal of Democracy* 21, no. 3 (June): 69-83. https://www.journalofdemocracy.org/articles/liberation-technology/.

DW. 2018. "Google reportedly working on censored search engine for China." DW. https://www.dw.com/en/google-reportedly-working-on-censored-search-engine-for-china/a-44923838.

Fayoyin, A., and E. Ngwainmbi. 2015. "Use and misuse of data in advocacy, media and opinion polls in Africa: Realities, challenges and opportunities." *Journal of Development and Communication Studies* 3, no. 2 (March). https://www.ajol.info/index.php/jdcs/article/view/112465.

Feldstein, Steven. 2019. "How Artificial Intelligence Is Reshaping Repression." Carnegie Endowment for International Peace. https://carnegieendowment.org/2019/01/09/how-artificial-intelligence-is-reshaping-repression-pub-78093.

Feldstein, Steven. 2020. "Revitalizing Democracy: Digital Democracy Struggles - The Day After." Carnegie Endowment for International Peace. https://carnegieendowment.org/2020/09/09/digital-democracy-struggles-pub-82532.

Feldstein, Steven. 2021. "How Digital Repression Is Changing African Politics." Democracy in Africa. http://democracyinafrica.org/how-digital-repression-is-changing-african-politics/.

Fingas, J. 2019. "51 companies tell Congress it's time to tackle data privacy." Engadget. https://www.engadget.com/2019-09-10-tech-companies-ask-congress-for-data-privacy-law.html.

Franz, Erica, Andrea Kendall-Taylor, and Joseph Wright. 2020. "Digital Repression in Autocracies." V-Dem. https://v-dem.net/media/publications/digital-repression17mar.pdf.

Freedom House. 2019. "Zimbabwe: Freedom on the Net 2019 Country Report." https://freedomhouse.org/country/zimbabwe/freedom-net/2019.

Freedom House. 2021. "Uganda: Freedom on the Net 2021 Country Report." https://freedomhouse.org/country/uganda/freedom-net/2021.

Gambardella, Jep, and Mandira Bagwandeen. 2021. "Don't blame China for the rise of digital authoritarianism in Africa." LSE Blogs. https://blogs.lse.ac.uk/africaatlse/2021/09/09/dont-blame-china-for-rise-of-digital-authoritarianism-africa-surveillance-capitalism/.

Gargiulo, Michael. 2021. "Which Countries Block VPNs, And Why?" VPN.com. https://www.vpn.com/guide/which-countries-block-vpn/.

Gillwald, Alison. 2018. "Understanding the Gender Gap in the Global South." After Access. https://afteraccess.net/wp-content/uploads/2018-After-Access-Understanding-the-gender-gap-in-the-Global-South.pdf.

GSMA. 2018. "Mandatory Registration of Prepaid SIMs | Mobile Policy Handbook." https://www.gsma.com/publicpolicy/mobilepolicyhandbook/mandatory-registration-of-prepaid-sims.

GSMA Connected Women. 2021. "The Mobile Gender Gap Report 2021." GSMA. https://www.gsma.com/r/wp-content/uploads/2021/07/The-Mobile-Gender-Gap-Report-2021.pdf.

Hale, Lee, and Eyder Peralta. 2021. *NPR*, October 15, 2021. https://www.npr.org/2021/10/15/1046106922/social-media-misinformation-stokes-a-worsening-civil-war-in-ethiopia.

Hamilton, Isobel A. 2022. "Internet censorship cost the global economy $5.5 billion in 2021, report says." Business Insider. https://www.businaessinsider.com/internet-shutdowns-cost-global-economy-5-billion-2021-report-2022-1?r=US&IR=T#:~:text=Internet%20shutdowns%20cost%20the%20global,80%25%20from%202020%20to%202021.

Hersey, Frank. 2021. "Centralized, decentralized or neither: which national digital ID system will you choose?" Biometric Update. https://www.biometricupdate.com/202112/centralized-decentralized-or-neither-which-national-digital-id-system-will-you-choose.

Higman, Susan, Vikas Dwivedi, Alpha Nsaghurwe, Moses Busiga, Hermes S. Rulagirwa, Dasha Smith, Chris Wright, Ssanyu Nyinondi, and Edwin Nyella. 2018. "Designing interoperable health information systems using Enterprise Architecture approach in resource-limited countries: A literature review." *International Journal Health Planning Management* 34 (July): e85-e99. https://pdf.usaid.gov/pdf_docs/PA00TM1R.pdf.

ID4Africa. 2019. "Roundtable of African Data Protection Authorities: Proceedings of a Workshop." *ID4Africa 5th Annual Conference*, (June). https://www.id4africa.com/2019/files/RADPA2019_Report_Blog_En.pdf.

IDEA. 2021. "THE GLOBAL STATE OF DEMOCRACY 2021 Building Resilience in a Pandemic Era." https://www.idea.int/gsod/sites/default/files/2021-11/the-global-state-of-democracy-2021_1.pdf.

Ilori, Tomiwa. 2020. "Data protection in Africa and the COVID-19 pandemic: Old problems, new challenges and multistakeholder solutions." African Internet Rights and Freedoms. https://www.apc.org/en/pubs/data-protection-africa-and-covid-19-pandemic-old-problems-new-challenges-and-multistakeholder.

Ingram, Mathew, and Amanda Darrach. 2021. ""A determining role"? Myanmar refugees sue Facebook." Columbia Journalism Review. https://www.cjr.org/the_media_today/myanmar-refugees-sue-facebook-for-150-billion.php.

International Bar Association. 2021. "The IBA African Regional Forum Data Protection/Privacy Guide for Lawyers in Africa." https://www.ibanet.org/Africa-IBA-releases-data-protection-guide-for-African-lawyers.

Johnson, Adetokunbo. 2021. "Human Rights and the Gender Digital Divide in Africa's COVID-19 Era." Global Campus of Human Rights. https://gchumanrights.org/preparedness/article-on/human-rights-and-the-gender-digital-divide-in-africas-covid-19-era.html.

Kaufman, Robert, and Stephan Haggard. 2021. *Backsliding: Democratic Regress in the Contemporary World*. N.p.: Cambridge University Press.

https://www.cambridge.org/core/elements/abs/backsliding/CCD2F28FB63A56409FF8911351F2E937.

Kujawski, Mike. 2019. "Misinformation vs. Disinformation vs. Mal-information | by Mike Kujawski." Medium. https://medium.com/@mikekujawski/misinformation-vs-disinformation-vs-mal-information-a2b741410736.

Makananise, Fulufhelo O., and Shumani E. Madima. 2020. "The use of digital media technology to promote female youth voices and socio-economic empowerment in rural areas of Thohoyandou, South Africa." *Gender and Behaviour* 18, no. 2 (July). https://www.ajol.info/index.php/gab/article/view/198213.

Makinen, Maarit, and Mary Wangu Kuira. 2008. "Social Media and Post-Election Crisis in Kenya." *Information & Communication Technology - Africa* 13. https://repository.upenn.edu/cgi/viewcontent.cgi?article=1012&context=ictafrica.

Makoye, Kizito. 2021. "Tanzania struggles to dispel myths against COVID-19 vaccines." Anadolu Agency. https://www.aa.com.tr/en/africa/tanzania-struggles-to-dispel-myths-against-covid-19-vaccines/2336356.

Menocal, Alina R. 2021. "Digital technologies and the new public square: revitalising democracy?" Democracy in Africa. http://democracyinafrica.org/digital-technologies-and-the-new-public-square-revitalising-democracy/.

Mhlanga, Carol, Taruvinga Muzingili, Cornelius Dudzai, and Johanne Mhlanga. 2021. "Information enclave and corona virus disease 2019 (COVID-19) pandemic in remote areas: a case of Binga district, Zimbabwe." *African Journal of Social Work* 11, no. 4 (October). https://www.ajol.info/index.php/ajsw/article/view/215414.

Musoke, Ronald. 2019. "Misusing computer misuse law." *The Independent* (Kampala, Uganda), August 5, 2019. https://www.independent.co.ug/misusing-computer-misuse-law/.

NORC at the University of Chicago and Simon Migliano. 2021. "Digitized autocracy literature review : final report." USAID Bureau for Democracy, Conflict and Humanitarian Assistance. Center of Excellence on Democracy, Human Rights and Governance. https://pdf.usaid.gov/pdf_docs/PA00XV9R.pdf.

Nwafor, Gloria. 2020. "Africa to harmonise laws for data protection, digital economy." The Guardian Nigeria. https://guardian.ng/appointments/africa-to-harmonise-laws-for-data-protection-digital-economy/.

Ojango, Stella Musembi, Annette Kwamboka Akama, Emmanuel Otieno Ouma, and Michael Njuguna Kamau. 2021. "Cybersecurity 2021 - Kenya." Chambers and Partners. https://practiceguides.chambers.com/practice-guides/cybersecurity-2021/kenya/trends-and-developments.

Okunoye, Babatunde. 2020. "Understanding the use of tools during Internet censorship in Africa: Cameroon, Nigeria, Uganda and Zimbabwe as case studies." Open Technology Fund Information Controls Fellowship. https://research.torproject.org/techreports/icfp-censored-continent-2020-07-31.pdf.

OSCE. 2019. "#SOFJO Safety of Female Journalists Online." The OSCE Representative of Freedom of the Media. https://www.osce.org/files/f/documents/2/5/370331_0.pdf.

Owono, Julie. 2018. "Atteinte à la liberté d'expression au Mali : sommes-nous encore dans une démocratie ? - sahelien.com." Sahelien.com. https://sahelien.com/atteinte-a-la-liberte-dexpression-au-mali-sommes-nous-encore-dans-une-democratie/.

Paul, Kari. 2022. ",Game of Whack-a-Mole': why Russian disinformation is still running amok on social media." The Guardian. https://www.theguardian.com/media/2022/mar/15/russia-disinformation-social-media-ukraine.

Privacy International. 2020. "Here's how a well-connected security company is quietly building mass biometric databases in West Africa with EU aid funds." https://privacyinternational.org/news-analysis/4290/heres-how-well-connected-security-company-quietly-building-mass-biometric.

Raman, Anand, and Greg Chen. 2017. "Should Other Countries Build Their Own India Stack?" CGAP. https://www.cgap.org/blog/should-other-countries-build-their-own-india-stack.

RAN Lab. 2019. "Understanding the Benefits, Costs, and Challenges of the National Identification System in Uganda." *USAID and the ResilentAfrica Network (RAN) at the Makerere University School of Public Health*, (December). https://www.ranlab.org/wp-content/uploads/2020/10/Understanding-the-Benefits-Costs-and-Challenges-of-the-National-Identification-System-in-Uganda-1.pdf.

Roberts, Tony. 2021. "Digital Rights in Closing Civic Space: Lessons from Ten African Countries." Institute of Development Studies. https://www.ids.ac.uk/publications/digital-rights-in-closing-civic-space-lessons-from-ten-african-countries/.

Roberts, Tony. 2021. "Surveillance Law in Africa: a review of six countries." Institute of Development Studies. https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Roberts_Surveillance_Law_in_Africa.pdf?sequence=1&isAllowed=y.

Schoemaker, Emrys. 2021. "The Taliban are showing us the dangers of personal data falling into the wrong hands." The Guardian. https://www.theguardian.com/global-development/2021/sep/07/the-taliban-are-showing-us-the-dangers-of-personal-data-falling-into-the-wrong-hands.

Schubert, Ingo. 2021. "New Technology in Europe's COVID Certificates." SecurID. https://www.securid.com/en-us/blog/2021-09/the-new-technology-powering-european-covid-certificates.

Sullivan, David. 2020. "Five Ways Telecommunications Companies Can Fight Internet Shutdowns." Lawfare Blog. https://www.lawfareblog.com/five-ways-telecommunications-companies-can-fight-internet-shutdowns.

Tavaana. n.d. "Ushahidi: From Crisis Mapping Kenya to Mapping the Globe." Accessed December 28, 2021. https://tavaana.org/en/en/content/ushahidi-crisis-mapping-kenya-mapping-globe.

UNESCO. 2020. "Disinfodemic: deciphering COVID-19 disinformation." UNESDOC Digital Library. https://www.frontiersin.org/articles/10.3389/fcomm.2020.00045/full.

USAID. 2018. "How To: Create Digital ID for Inclusive Development." https://www.usaid.gov/sites/default/files/documents/15396/DID_Layout_v9_Interactive.pdf.pdf.

USAID. 2020. "The Gender Digital Divide Primer." USAID. https://www.usaid.gov/sites/default/files/documents/DAI-1089_GDD_Primer-web_rev1_9.6.21.pdf.

USAID. 2021. "Disinformation Primer." Center of Excellence on Democracy, Human Rights and Governance. https://pdf.usaid.gov/pdf_docs/PA00XFKF.pdf.

USAID. 2021. "Digital Ecosystem Framework." USAID. https://www.usaid.gov/digital-development/digital-ecosystem-framework.

USAID. 2021. "Cybersecurity Primer." USAID. https://www.usaid.gov/sites/default/files/documents/10-26-21_EXTERNAL_CyberPrimer-CLEARED-accessible.pdf.

USAID. 2022. "USAID Digital Strategy." https://www.usaid.gov/digital-strategy.

V-Dem Institute. 2021. "Pandemic Backsliding: A Year of Violations and Advances in Response to COVID-19." Policy Brief. https://www.v-dem.net/media/publications/pb_32.pdf.

Wasuna, Brian, and Joseph Wangui. 2021. "Judge orders State to regularise Huduma Namba roll out." The Nation. https://nation.africa/kenya/news/judge-orders-state-to-regularise-huduma-namba-roll-out-3582906.

Wilhelm, Jan P. 2018. "Internet censorship in Africa threatens democracy, economy | Africa." DW. http://dw.com/en/internet-censorship-in-africa-threatens-democracy-economy/a-44956169.

USAID
FROM THE AMERICAN PEOPLE