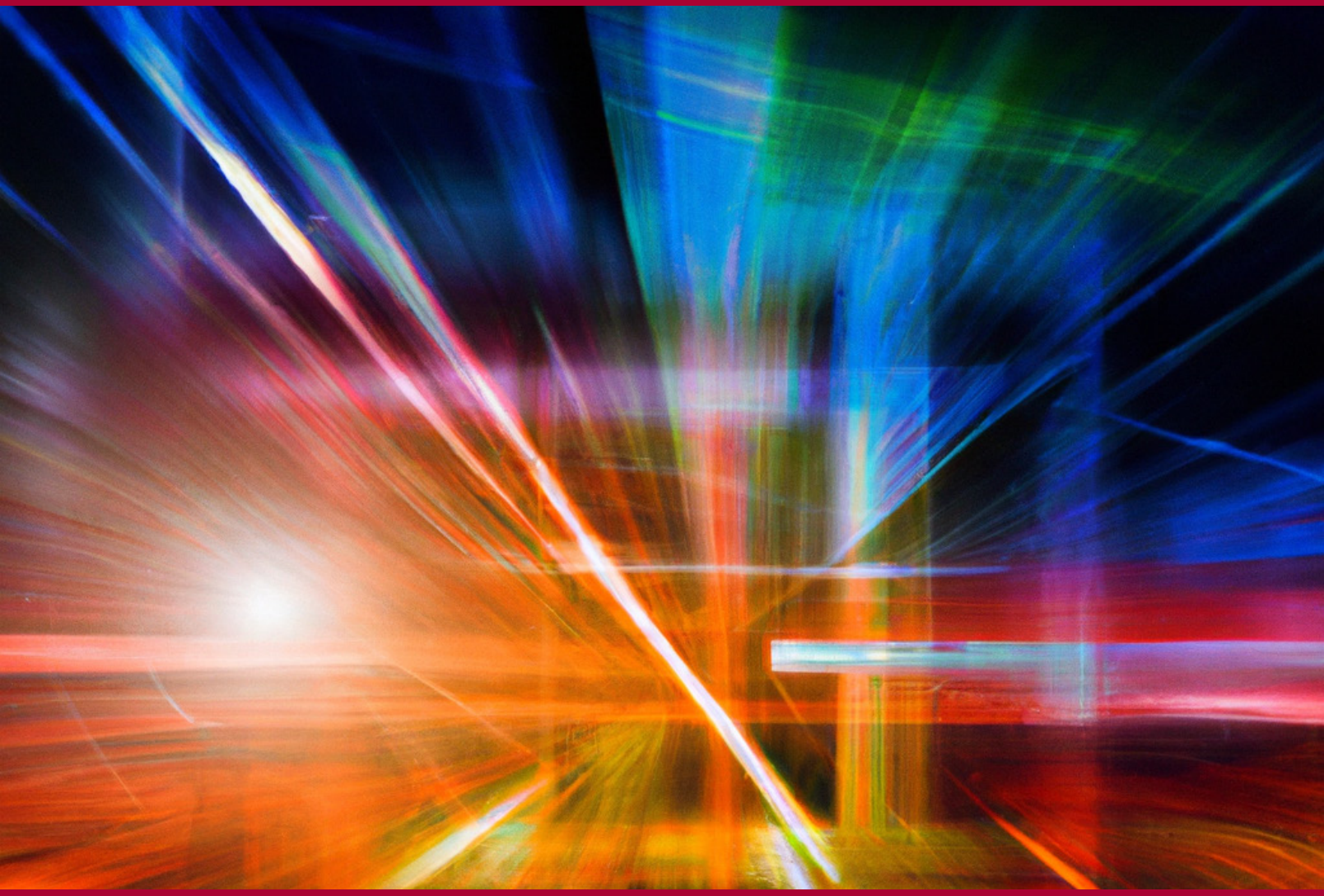
Digital Technologies in Emerging Countries

Edited by Francis Fukuyama and Marietje Schaake



Stanford | Cyber Policy Center
Freeman Spogli Institute and Stanford Law School

Contents

Introduction

Over much of the past decade, there has been an intense focus on the impact of digital technologies on politics and society, and particularly on their impact on contemporary democracy.

When the internet was first privatized in the 1990s, there was great optimism that it would constitute a "liberation technology" that would empower ordinary people to inform themselves, mobilize, and ultimately become participating agents in a democratic process. Digital technologies have in fact played that role in many parts of the world, supporting democratic mobilizations, offering new paths to economic growth, and providing educational opportunities to many who earlier lacked access.

But as time went on, it became clear that digitization was a two-edged sword and could have highly deleterious consequences for both democratic politics and societies more broadly. The assumption that the internet would inevitably erode an authoritarian government's control of its populace was disproven by China, which succeeded in cutting off the great majority of its citizens from the global internet and in using new technologies to exert an unprecedented level of control over its own population. Russia, for its part, was an early innovator in the weaponization of social media, using it as a tool for undermining the trust of citizens of rival states in their own governments.

Quite apart from these geopolitical developments, there was a growing realization that the internet, and social media in particular, was having other malign consequences for modern societies. The enormously successful business models of the big social media platforms—Google, Facebook (now Meta), Amazon, Microsoft, Apple, and Twitter—were built around the use of personal data to target advertising. In effect, they were monetizing their ability to compromise their users' privacy. These private corporations had a strong incentive to prioritize viral content, often at the expense of credibility or concern for social impacts. Moreover, their possession of vast amounts of user data gave them an intrinsic advantage when moving into new sectors, and saw them overwhelm competitors and grow to unprecedented size in global scale and scope. The shift to online commerce undermined physical interactions, emptied downtowns, and created huge problems for cybersecurity.

Social media also abetted the rise of populist nationalist movements within established liberal democracies, beginning with the United States: the 2016 presidential election that brought Donald Trump to power was a wake-up call to the polarizing impact of digital platforms, and their unprecedented ability to micro-target specific populations and expose them to disinformation. This practice continued through the 2020–22 COVID-19 pandemic, where online communications made economic activity possible for many people, but also saw the rise of disinformation campaigns surrounding public health and the subsequent politicization

of formerly uncontroversial issues like vaccinations.

In addition, the period of the COVID-19 pandemic has revealed and in many ways exacerbated social inequalities, both within societies and between them. Developed countries with large service sectors saw highly paid professionals moving online and away from urban areas due to social distancing during the pandemic, while working-class people in manufacturing or service sector jobs like hospitality or retail saw their livelihoods disappear. Many emerging countries with weak digital infrastructure saw their children lose a few years of schooling as educational institutions shut down and students were stranded at home without access to computers or the internet.

While there has been a tremendous upsurge in scholarly research into the political and social impacts of digital technologies, the vast majority of this work has tended to focus on rich countries in North America and Europe. Both regions had high levels of internet penetration and the state capacity to take on—potentially, at any rate—regulatory issues raised by digitization. The United States, of course, was home to Silicon Valley and the source of many of the new disruptive technologies that were reshaping politics. By the middle of the 2010s, it was also falling into a political crisis caused by rampant political polarization and rising populism. As a result, there was growing political pressure directed particularly at the big platforms to better police the content they carried. It is not surprising, therefore, that much of the early research and scholarship on the impact of digital technologies and potential public policy responses has focused on these developed regions. This was reflected in the fact that in 2020 roughly 80% of Facebook's growing budget for content moderation was devoted to the United States, leaving the remaining 20% to police the world's other 180-some countries.

Programs, including many funded by the Knight Foundation, were established across the United States to gather empirical data on the new emerging digital world and to analyze it rigorously. Stanford University's Freeman Spogli Institute for International Studies created a Cyber Policy Center in 2019 to look at the political, economic, and policy dimensions of digitization. Within that new center, the Program on Democracy and the Internet sought to focus particularly on the challenges that digitization poses to democratic institutions, such as disinformation, toxic content, hate speech, platform scale, approaches to content moderation, and the like.

The current volume is an initial effort to rectify the imbalance in the way that centers and programs such as ours look at the world, by focusing on what might broadly be labeled the "global south," which we have labeled "emerging countries" (ECs). Countries and regions outside of North America and Europe face similar opportunities and challenges to those developed regions, but also problems that are unique to themselves.

The current volume is an initial effort to rectify the imbalance in the way that centers and programs look at the world, by focusing on emerging countries.

For example, as in the global north, many countries in the global south face the problem of weaponized disinformation, and the use of social media to sway political outcomes not so much through old-fashioned propaganda, but through a more subtle discrediting of opponents or the propagation of false narratives. However, the political balance between state and society is often quite different. As in the United States, individual politicians, beginning with Donald Trump, have used social media to broadcast their views and attack opponents. Trump was banned from Twitter and other social media platforms after January 6, 2021, not as the result of a state edict, but rather as the result of social pressure and the preferences of the platform owners themselves. But in the EC world, the state itself often plays a more direct role in shaping social media discourse, often by forcing the platforms to take down disapproved content in a non-transparent way. In addition, the predominant platforms used by EC citizens are often different: in many countries, encrypted messaging services like Telegram, Signal, or WhatsApp are used in preference to more open platforms like Twitter or Facebook. This potentially creates greater obstacles for government censors, but ones that governments can work around creatively.

A second issue for ECs has to do with what might be called "digital colonialism." The vast majority of popular platforms have been based in the United States, where Americans or their local agents were put in charge of content moderation. In the United States, platform behavior could be shaped directly by social and political pressure, while in Europe, the size of the European market gave EU regulators leverage over the platforms. While the US has been reluctant to regulate the platforms directly, the same is not true for Europe, which has issued major directives like the General Data Privacy Regulations (GDPR) or the Digital Services Act.

ECs, by contrast, often lack both market size and state capacity to be able to influence platform behavior. This is not true in large countries like China or India, which have succeeded in establishing their own regulatory regimes, but is definitely the case for smaller countries in Africa, Asia, and Latin America. Some have found themselves at the mercy of decisions taken in the U.S., while others have seen the platforms' lack of attention and local knowledge as an opportunity for shaping the information space.

The issue of the power imbalance between the U.S. and Europe, on the one hand, and ECs on the other, plays out also in the realm of international regulation. At the birth of the internet, existing regulation such as the Internet Corporation for Assigned Names and Numbers (ICANN) was taken out of the hands of older regulatory bodies like the International Telecommunications Union (ITU) and run by Americans (indeed, at the beginning this function was exercised by a single American graduate student). Many ECs contested the legitimacy of this arrangement, and there has subsequently been a struggle both to broaden the ICANN's governance, and to bring international regulation back more generally under the authority of the ITU. Related to this is an ongoing struggle for control of the ITU itself.

"Digital colonialism" isn't a simple matter of U.S. dominance. A third and related issue for ECs is the growing geopolitical rivalry between the U.S. and China, and the latter's efforts to extend its influence via the "digital Belt and Road." The emergence of Chinese companies like Huawei and ByteDance (the parent of TikTok) is both an opportunity and threat. Many emerging countries now have multiple options for technology providers, and can play Chinese and Western companies and governments against one another. On the other hand, there are fears about Chinese export of surveillance technology, which has been used in China itself through the PRC's social credit and COVID-19 surveillance systems. This capacity, of course, is at times welcomed by governments in ECs, which want to be able to exercise greater control over their citizens. Others, like India, have followed the U.S., Australia, and other Western countries in blocking Chinese hardware companies and the use of Chinese apps.

A fourth issue for ECs has to do with new, cutting-edge technologies that have been introduced in recent years and whose use will expand rapidly in the near future, like artificial intelligence and cryptocurrencies based on blockchain technology. As we are preparing this volume, the crypto world has come under intense scrutiny with the collapse of the FTX trading platform and the broad decline in cryptocurrency values in the course of 2022. For many Americans and Europeans, cryptocurrencies seemed to be a solution in search of a problem. While they were supposed to be a hedge against inflation, they declined in value even as inflation rekindled through much of the world. Yet there are ECs with weak banking institutions and untrustworthy governments, for which blockchain may actually be a useful technology.

Artificial intelligence has been put to use by the big technology

platforms for some time now, and stands to become an increasing threat to privacy as it is used in surveillance technology and other forms of data-gathering. There are plenty of new uses for AI over the horizon, such as in the production of deep fakes that have obvious malign political uses and threaten to further undermine trust in politics. Unlike other forms of high-tech, these types of AI are low cost and likely to spread quickly across much of the world.

Finally, it is important to note the positive contributions that digital technologies have and can make to better democratic governance and greater social inclusion. Through their cellphones and other devices, hundreds of millions of people in ECs now have access to the internet and the information it provides. All of this contributes to economic growth and opens up new opportunities for greater democratic accountability. From the beginning, the great hope was that the internet would democratize access to information and promote positive social mobilization, and it continues to perform these functions even as malign actors misuse its capabilities.

Contributions to the current volume touch on many of these issues, and provide perspectives on how digital technologies are used, perceived, and affect behavior in a range of countries outside of North America and Europe. This volume should be seen as a modest first effort to gather comparative data on digital technology issues affecting ECs that will inform government policy, the platforms, and civil society around the world.

Francis Fukuyama
Stanford University
Olivier Nomellini Senior Fellow, Freeman Spogli Insitute
Director, Ford Dorsey Master's in International Policy

Disinformation, The Weaponization of Social Media, and Digital Regulation

Chat Apps, Mass Mobilization, and Authoritarian Control: Assessing Evidence from Egypt, Iran, and Morocco

Inga Kristina Trauthig

ABSTRACT:

Researchers and policymakers alike have acknowledged the recent trend of digital authoritarianism, but coherent ways to halt this trend are still lacking. One technology that is charged with hope for civil society and democratic activists in authoritarian countries is end-to-end encryption (E2EE). This paper addresses four main questions while focusing on Egypt, Iran, and Morocco: Are encrypted messaging apps (EMAs) important for online political communication? Are EMAs important to organize offline political activities? What challenges to the countries' regimes are arising from this type of internet usage? How are the regimes responding?

The paper argues that encryption is only relatively successful in furthering democratic pushback to authoritarian developments, because even if regime forces might not have the technical capabilities to access discussions on EMAs, the societal fear, uninterest, or skepticism keeps many activists from forming movements. At the same time, EMAs have developed into an important platform for journalists as the main technological facilitators for ad hoc politicization. Therefore, it is important to protect and assist local populations trying to communicate securely and speak freely about politics. The last part of the paper outlines how Western policymakers could support this—one key point being that economic cuts might need to be accepted if the cyberspace is included in holistic policy development and enforcement.

KEYWORDS: Authoritarian resilience, social movements, encrypted messaging apps.

1 INTRODUCTION

By 2022, the notion that the internet would manage to challenge or even threaten authoritarian regimes seemed long outlived (Buchanan, 2015). In retrospect, the Arab Uprisings of 2011 were an exception to the norm of authoritarian regimes managing to control the potential political impact of internet use that would result in mobilization of the masses (Ali & Fahmy 2013; Hussain, 2014; Moore-Gilbert & Abdul-Nabi, 2021). However, both the notion that authoritarian governments are in full control of "the internet" as well as the belief that emerging technologies alone can change the nature of a political system are simplistic.

This paper assesses how the rise of chat apps that often rely on end-to-end encryption (E2EE) affects popular mobilization as citizens carve out spaces to discuss politics more freely

Disinformatio

and organize politically via these platforms (Attia, 2021). With this, the paper challenges existing scholarship that largely denies that more intimate spaces with smaller reach like encrypted messaging apps (EMAs) have the potential for mass mobilization due to their platform features (Enjolras et al., 2013; Onuch, 2014). The results have implications for the balance of power between exclusionary states (regimes) and respective societies.

The paper has three aims:

- Establish that EMAs have risen in importance for online political communication and its offline impacts such as protests or other political activities.
- Assess what challenges to the countries' regimes are arising from this type of internet usage and how the regimes are responding.
- Deliver insights into the likelihood of mass mobilization in Egypt, Iran, and Morocco based on the research findings.

The study focuses on three authoritarian regimes in emerging countries—Egypt, Iran, and Morocco—that largely maintain control over the internet's political impact through various combinations of reactive but also proactive strategies (Bitso et al., 2013; Murdoch & Roberts, 2013). Among the reactive strategies are (1) filtering content or blocking platforms, (2) monitoring users' online behavior (with spyware, as well), and (3) shutting down the internet, albeit for limited periods of time. Among the proactive strategies assessed are (4) distributing state propaganda domestically, (5) establishing state-controlled intranets, or (6) strengthening state power on an international scale by engaging in information warfare. All these efforts are related to the degree of state capacity generally, but some also require particular prerequisites such as state control over infrastructure (Wagner, 2012; Zeitzoff, 2017). The latter is best achieved in Iran; it is also achieved in Egypt, but barely in Morocco (Ibahrine, 2003; Oxford Business Group, 2017; The Economic Intelligence Unit, 2008).

While Section 2.1 discusses how EMAs are used for discussing and organizing political action, Section 2.2 focuses on three of the authoritarian regimes' strategies listed above: (1) filtering content or blocking platforms and (2) monitoring users' online behavior, as well as (4) distributing state propaganda domestically, since these strategies are most directly related to EMAs and applied in all three case studies, albeit with varying success. The paper argues that EMAs are characterized both by liberatory (contributing to democratic activism) and oppressive (contributing to authoritarian resilience) uses—overall, these platforms have also developed into important means for political communication. Importantly, EMAs have developed into a crucial tool for ad hoc mobilization, which could spill over into bigger movements if other factors come together as they did in 2011. This has implications for policymakers, researchers, civil society, and platform and app designers, all of whom would need to think critically about both the democratizing and the misinformative uses of emerging internet tools and applications.

EMAs have developed into a crucial tool for ad hoc mobilization.

1.1 CASE STUDY SELECTION

The selection of Egypt, Iran, and Morocco as case studies for this paper relied on three main factors: (a) their political systems and hence their push factors for political mobilization; (b) specific features of these systems and hence their pull factors, and (c) the prominence of EMAs in all three countries and hence their wide reach.

a. All three countries are designated non-democracies or "hardline autocracies" (Bertelsmann, 2022a). Therefore, the research questions of potential new avenues for free speech and democratic organizing are pertinent. But they vary in their performance with regard to governance (removed from institutional set-ups): Morocco's performance is "moderate," Egypt's is "weak," and Iran's a "fail" (Bertelsmann, 2022b). This matters, because these performance indicators serve as reference points for social movements scholars interested in the dynamics of mass mobilization. In this view, Iran has the biggest push factor.

b. While displaying similar structures, the three countries govern with differing levels of authoritarianism and have differing controls of different parts of the internet—Egypt and Iran are classified as "not free" and Morocco as "partly free" (Freedom House, 2021a). Furthermore, Access Now and the #KeepItOnCoalition recorded internet shutdowns in both Egypt and Iran but none in Morocco in 2020 (Freedom House, 2021a). These pull factors can help to distill both similarities and variations when addressing the research questions, such as whether higher levels of authoritarianism increase the population's reliance on EMAs for discussion of political matters (or whether higher levels of authoritarianism instill so much fear that political discussions are also avoided on EMAs).

c. In Egypt, Telegram is the most popular app according to downloads, WhatsApp third, with Signal falling behind at 44th place (Similar Web, 2021). In Iran, over 60% of the population use WhatsApp and over 30% Telegram—which is banned (ISPA, 2021). In Morocco, over 80% of the population use WhatsApp, and Telegram has been the fourth most-used social media platform in 2021 (Morocco News, 2021; Statista, 2021).

While there are other countries that fit the above criteria (a, b, and c), the selection of only three cases fits the qualitative research design that aims for in-depth comparison of a few cases, instead of covering broader trends for many. The ultimate aim, however, is to integrate the insights from this research into a bigger research project. Finally, the three countries share joint characteristics: all three have seen popular uprisings in the form of joint protests or individual civil unrest in the recent past—albeit of varying degree and background—(Debackere & Akouh, 2021; Hamidi, 2021; Magdi, 2020), and all three have colonial histories that still define relations and attitudes toward the West and its democratic ideals (Frampton, 2018).

2 FINDINGS

2.1 RESEARCH QUESTION 1:

Are EMAs used to discuss politics online and organize offline political action in authoritarian states?

Eleven years later, it is safe to say that the Arab Uprisings captured a new trend of mobilization that scholars would regard as modern, decentralized, "networked" social movements (Castells, 2012; Chu, 2018; Gerbaudo, 2012). Largely, however, scholarship revolves around features of these networked social movements (inter alia opaque leadership or the importance of social media generally). Fewer academics aim to distill which platforms are used for what type of political discussion—or even more importantly, which platforms hold relevance for which type of political action (Farrel, 2012; Frosina, 2021; Lee et al., 2021; Urman et al., 2020; Walker, 2020; Weidmann & Rød, 2019).

2.1.1 Data Collection and Results

In order to have an empirical background for assessment, we built a database that captures (a) protests and other reported political activity in the three countries and (b) evidence that EMAs were used to organize but also discuss these political activities.[1] The development of this database goes hand in hand with semistructured interviews and existing research

1 For this database, I and other researchers affiliated with the Propaganda Research Lab team systematically searched news aggregation websites such as www.maghress.com and www.masress.com as well as LexisNexis in English, French, Arabic, and Persian. I cross-referenced all entries to rely on at least two data points for every entry in the database. Additional data was collected using open-source-based research tools, such as TweetDeck and Facebook Search. All searches were guided by a keyword list in English, French, Arabic, and Persian—some searches combined with operators—that remained the same throughout the research period. Given the study's focus, retweets or shares picking up the recorded political activity were not included in the count. Comments on the political activities, however, were considered in the analysis. The data collection period covers January 1, 2020, until March 31, 2022. During this period, all newspaper articles, Tweets, and Facebook posts were collected that claimed political activity in Egypt, Iran, and Morocco in the following areas: (1) protests, (2) boycotts, and (3) formation of political association or party; all three are forms of public mobilization against the government. Conversely, this means other ways of political expression did not make it into the database, most markedly among them online campaigns or political violence. The decision not to include those activities was taken because the evidence of online campaigns, while significant in itself, is little helpful when assessing offline impact; political violence was not included because this type of radicality is exerted by fringe movements rather than larger parts of the population. However, assessments of these activities have

TABLE 1. Overview of recorded political activity based on the authors' data collection.

COUNTRY	RECORDED 1/1/2020–3/31/2022
Total Incidents	52
Egypt	19
Iran	22
Morocco	11

by the Propaganda Research Lab in the Center for Media Engagement at UT Austin, which captured the increasing politicization of EMAs in Southeast Asia as well as in some diaspora communities in the U.S. (Gursky, et al., 2020; Martin, et al., 2021; Trauthig & Woolley, 2022). For the database, the reliance on open-source methods adds to the traceability and replicability of the research. However, this approach also has limitations, as it can only record publicly available information. In order to address these limitations, our team conducted additional qualitative interviews that are factored into any follow-up analysis. RQ1 functions as a premise for RQ2: the rise of chat apps relying on end-to-end encryption (E2EE) affects popular mobilization as citizens carve out spaces to discuss politics more freely and organize politically on these platforms.

As Table 1 shows, during the 27-month data-collection period, a total of 52 incidents ended up in the database, broken down into the three case studies of Egypt, Iran, and Morocco and fulfilling the defined inclusion criteria. Iran leads with the most recorded incidents, which is surprising as the country is considered the least free of all three case studies. A total of 22 events were recorded, with a regional concentration in Tehran. For Morocco, the Rif region was responsible for over half of the recorded incidents; in Egypt, Cairo had the most activities, albeit if political violence had been included, the Sinai Peninsula would have been the most significant area.

In addition to recording those political activities generally, the database shed light on the importance of EMAs for political resistance in authoritarian regimes. Based on the data gathered via open-source methods, 9 of the 19 political activities in Egypt were organized or discussed on EMAs; for Iran, the breakdown is 17 of 22, and for Morocco, 4 out of 11. In total, that is 57.7% of all recorded political activities. The breakdown is a first indication confirming the hypothesis that the more authoritarian a state, the more important EMAs are for political discussion and organization, as Iran is the most authoritarian state with the highest percentage of EMA relevance for political activities.

2.1.2 Interview Findings[2]

While the descriptive numerical analysis above was focused on collecting the number of incidents, type of activity, and relevance of EMAs, which already carries weight in terms of (non)existing political activities in those authoritarian states, qualitative analysis is needed to provide additional analytical depth. Interviewees were selected based on their activism or background working in the areas of journalism, research, and/or civil society organizations (especially fact-checking organizations) in the respective countries. Most of the interviewees are still based in those countries, while others lived there for many years but recently joined the diaspora. The 19 interviews focused first on the self-described importance of EMAs by civil society activists in those countries and second on the differentiation between

been and will continue to be included in this paper, as such activities provide valuable, additional glimpses into political unrest in those countries.

2 Our team at CME has been conducting qualitative, semistructured interviews speaking to regional fact-checkers, journalists, civil society activists, and human-rights lawyers. The interviews are still ongoing, which might affect the portrayed main findings in this working draft. All interviewees are assigned pseudonyms to protect their identity.

different EMAs, with the aim of distilling imperial notions attached to different EMAs—most importantly WhatsApp as part of Meta's ecosystem, which dominates social media (Srinivasan, 2019). This second aspect developed as a research angle since our qualitative interviews were led by grounded theory, which helps findings to be led by the data rather than the theory preceding it (Glaser, 1992). Various interviewees mentioned how they used Telegram for the most secure communication—which is counterintuitive given that Telegram is not E2EE by default, like WhatsApp is. But they revealed this was the case because of concerns after Facebook's takeover of WhatsApp going hand in hand with general hesitancy toward U.S.-owned technologies (Karim, Roky, Stephanie—see Section 2.1.2). Generally, *all* our interviewees emphasized the importance of EMAs for news consumption as well as political discussion and organizing. This is a deviation from the above data, which captured 57.7% relevance. This discrepancy is best explained by some interviewees themselves, who regularly emphasized that as journalists and civil society activists they try to downplay the importance of EMAs in order to attract less state attention. This finding highlights the importance of qualitative research when studying less accessible platforms (versus, e.g., Facebook, YouTube, and Twitter) and their impact on societies. The interviews revealed three important themes: authoritarian resilience, murky information, and frustration release.

Authoritarian resilience

The social climate related to potential democratic change is pessimistic, and the conviction of the ubiquity of the state's security forces is widespread (Emad, Adel, Yasmine). While this general sentiment was also prevalent among the interviewed civil society activists and journalists, they try to make it as hard as possible for the state to monitor them. In the words of one journalist in Morocco, "I know the Mukhabarat is everywhere [but] I still try … some of them are old … it's easier for them to surveil me in cafes than the Internet" (Ala).

Here is where E2EE and EMAs manage to play a crucial role. The presence of the state on open social media platforms is well established, with officials and ministries running their own accounts (El-Khalili, 2013; Zarhloule, 2020). Therefore, activists would try to get people from talking about some topics on Facebook and to move that conversation to WhatsApp. For example, popular accounts sharing personal experiences as well as practical information about emigration from Morocco would post on Facebook first but then share their WhatsApp details in order to elaborate on more controversial issues (Herbert & Ghoulidi, 2020). These strategies, however, seem limited to activists and journalists; for the population writ large, "there is no awareness for operational security whatsoever … but some learn the hard way" (Emad). For political activism, the systematic realities of the regimes give little room for action. One Egyptian activist who joined the diaspora recently due to overbearing concerns about his personal safety in Cairo explained to us, "There is no offline activism. Period. … but activists rely on Signal [where] we can speak and plan inshallah" (Karim).

Out of the examined cases, the interview data pointed toward Morocco exhibiting the most room for potential political expression, as long as some red lines were not crossed; however, our database recorded the smallest number of political activities in the country. There is a larger macrodynamic overshadowing those existing possible avenues, namely depoliticization, which was mentioned by all interviewees in Morocco. This depoliticization is captured in a recent national survey with a representative sample of 1,500 citizens by the Moroccan Institute for Policy Analysis in which almost 50% expressed that they "do not follow politics at all" (Masbah et al., 2022).

Overall, these insights speak to the need for techno-skepticism in creating social movements and regime challenges, because even if security forces might not have the technical capabilities to access discussions on EMAs, societal fear, uninterest, or skepticism keep many activists from forming movements (Jeffries, 2013). This emphasizes the contributive, instead of central, nature of technologies to social mobilization: the technical affordances of these apps are not enough to motivate people in authoritarian contexts to form a movement. This assessment sets this analysis in 2022 apart from research undertaken shortly after the

Arab revolts in 2011 (Tufekci & Wilson, 2012). In addition, depoliticization and a well-known bargain that argues for relative security provided by the regime in exchange for obedience seems to have taken hold, especially in North Africa where Libya is referenced as a negative counterpoint. At the same time, EMAs have developed into the main technological facilitators for ad hoc politicization, e.g., protests in response to rising oil prices or sparked by water shortages in Iran's Khuzestan Province (Bahar, 2021), or boycotts against global food corporation Danone (Crooms, 2018).

Murky information ecosystems

EMAs developed into a relevant source for news consumption despite the murkiness of shared news items due to its often nonidentifiable origin. In all three case studies, official news channels on traditional as well as social media are well understood to be propaganda outlets of the regimes (Abdel, Aida, Naomi). This leads to a hunger for as many other news sources as possible. In Morocco and Egypt, Facebook in particular has been filling this need for years already (Schmidt et al., 2017). More recently, forwarding news articles (often PDF documents) and sharing any sort of breaking news (often without attached links, sources, or documents) has become a daily occurrence in Moroccan WhatsApp groups. Generally, news items often link to Arab online news sites of unclear origin and often temporary existence (Adel, Aida, Emad).

In Iran, a report by the Iranian Student Polling Agency from September 2021 claims that over 40% of students use social media and online media outlets as their main sources of news in the country (ISPA, 2021a, 2021b). Instagram seems to be particularly relevant to express controversial thoughts related to women's rights, for example (Einifar & Kosari, 2020). Ever since the mid-2010s, however, EMAs have proven their potential in news dissemination with attached rallying power. For instance, in the winter of 2017–18 demonstrations against the government were triggered by small groups of protesters in conservative Mashhadt, which were amplified on Telegram and circulated widely, leading to follow-up protests (Bayat et al., 2021).

Hand in hand with this change in sharing and distribution mechanisms for news, the level of trust on the recipient's end changes. In other words, EMAs are attributed with a higher level of intimacy by the user, which translates into a sort of prequalification of trustworthiness for anything shared via EMAs (Gursky et al., 2022; Trauthig & Woolley, 2022). Several interviewees expressed something similar to what one Moroccan activist captured in this sentence: "People believe: what is on WhatsApp is true" (Emad). Cross-platform infiltration is an important aspect for these dynamics, with Instagram a main source for snippets and short videos, as well as YouTube for (often longer) videos. Especially in Egypt and Morocco, Instagram influencers such as popular MMA fighters are successful in planting stories and influencing public opinion—their content is often then forwarded to EMAs (Borshchevskaya, 2021; Diwan, 2016; Ezzat, 2021).

Frustration release

EMAs developed into a new option for what Diamond (2010) argued is an accountability technology as part of social media's capacity as liberation technology. Proactively engaging on social media is considered a risky option for some politicians as they might be ridiculed. Many parliamentarians in Morocco, for example, are older, and some have direct examples of bad experiences with trying to engage with their electorate on social media. This largely seems to be a generational discrepancy between some politicians' ages and their knowledge about social media. Therefore, successful parties and individuals hire younger people to run accounts for them or pay existing influencers to promote their message (El-Khalil, 2013).

EMAs in particular have developed into popular fora to allow the forwarding of humoristic memes about the government, certain politicians, or policies (Dagres, 2022). The increased difficulty for regime censoring on EMAs due to barriers of accessibility is an underlying factor that helps regime-critical content to spread for longer than would be the case on open social media platforms. For example, Telegram was banned in Iran in 2018, and instead a domestic app called Soroush was promoted as an alternative (CHRI, 2018). Shortly after the ban, a clip was circulated widely on EMAs that showed an

Iranian couple messaging and sharing pictures on Soroush, with an officer from the security services interfering in the chat and inserting his own selfie (Dagres, 2022).

2.2 RESEARCH QUESTION 2:

What challenges to the emerging countries' regimes are arising from this type of internet usage, and how are the regimes responding?

As a consequence of the above findings, two main challenges arise for the regimes directly related to EMAs: encryption and narrative control.

2.2.1 Encryption

Targeted attacks

In Egypt, the government is pursuing a crackdown on any voices that promote messages deemed threatening by President Sisi's regime. The state has also used forced disappearance and torture as methods of intimidation. Amnesty International (2020b, 2021a, 2022) has proven numerous times that instead of investigating police and military abuses, Sisi's regime appeases both entities. Breaches are defined broadly: a seemingly frustrated husband who runs a Facebook page on which he proclaims that 30% of Egyptian women are ready to cheat is also considered by the state as a threat to national security, relying on the well-known morality argument (Noureldin, 2016). Overall, the Sisi regime has built a repressive system that activists have described as manufacturing loyalty through fear—employing targeted online and offline attacks, misuse of draconian legislation, and relentless propaganda (Mohammad, Perri, Yasmine; Mandour 2022).

EMAs add a layer of protection for political discussion, but the regime attacks this layer of protection by conducting targeted attacks on individuals or organizations relying on acquired programs (Amnesty International, 2020a; Roky). In addition, different parts of the security apparatus hire external companies to monitor and then report online behavior of citizens, who are then prosecuted under draconian legislation. Especially in order to circumvent the added protection of EMAs, spyware programs need to be acquired or unethical infiltration mechanisms need to be employed to lurk in (larger) WhatsApp groups, for instance.

The regime's fears of losing control or at least insight/monitoring access with EMAs has been well understood in Morocco. The country hit the headlines in 2021 when a consortium around Citizen Lab revealed that Moroccan security services used the Pegasus spy software for targeted attacks into phones (Cohen, 2022; Kirchgaessner & Jones 2022; Marczak et al., 2018). Like other developing countries, Morocco is largely on the receiving end of technological developments and defined as a consumer more than a creator of platforms—this exacerbates the search for third-party services as well as monitoring systems—allowing the government to regain some control.

"We know that encryption is not torture proof. If I had been arrested, or kidnapped … no matter what kind of encryption you use, nothing will stand in front of this."

In Iran, security services arrested administrators of Telegram channels in 2017. In Egypt and Iran, "volunteers" monitor online activities and report anything suspicious. The interviewed activists were very aware of the intrusiveness and danger from the regime: "We know that encryption is not torture proof. If I had been arrested, or kidnapped, which has happened to the average activist in Egypt, no matter what kind of encryption you use, nothing will stand in front of this" (Roky).

Undermining encryption via legislation

These countries are aiming to give the described attacks

legal cover by creating legislation that justifies some of that intrusiveness. The rationales behind the legislation are largely claims of national security and related terrorism concerns (Trauthig, 2021). Another trend is to create legislation that rules out the dissemination of "fake news"—an extremely blurry term used to designate any information or claim the government disagrees with (Zimmermann & Kohring, 2018).

In summer 2021, another journalist, Abdel Naser Salama, was detained on both terrorism and false news charges, outlining the various tools at the disposal of Egypt's security forces when harassing activists (Holleis & Knipp, 2021). Morocco also has its version of "fake news" laws, but the regime has often relied on other legislation to intimidate activists (Freedom House, 2021b; Wiseman 2020). Online communications are restricted, e.g., with the Moroccan antiterrorism law from 2003, which gives the state wide-ranging authorities to filter and delete content that is deemed to "disrupt public order by intimidation, force, violence, fear, or terror."[3] In addition, the state of emergency Morocco imposed in March 2020 because of COVID-19 includes criminal penalties for content that contradicts the state of emergency (which is still ongoing at the time of writing in April 2022) (North Africa Post, 2022). Criticism of any state actions that might tie back to the King is interpreted broadly, and very few would take the risk to openly speak out about him—including on EMAs (Abdel, Emad, Yasmine).

As captured already, the governments are uneasy about the use of encryption tools, since they prevent monitoring and analyzing content, or at least make it more difficult. Therefore, a third avenue for legislation are laws restricting the use of encryption, which would threaten the use of EMAs for any communication (Bhardwaj, 2021; Tech Against Terrorism, 2022; WhatsApp, 2022). Iran introduced the "Cyberspace Users Rights Protection and Regulation of Key Online Services" bill in summer 2021, which would, inter alia, criminalize distribution, selling, and potentially using VPNs. VPNs have proven a crucial tool for Iranian society aiming to access platforms that the regime has banned, such as Telegram (CHRI, 2018). All tech companies offering email, hosting services, messaging, and social media in Iran would also need to name an Iranian representative to ensure compliance with the country's rules and collaborate on content moderation; existing sanctions make this extra difficult (Isfahani, 2021). Activists declare it obvious what this legislation is supposed to achieve: even further control with additional negative repercussions for the Iranian economy (Sarah). In addition to banning platforms, Iran has also tried to introduce apparent alternatives, e.g., to Telegram, when releasing Soroush or other apps like Bale or Gap. But even government agencies returned to Telegram after a hiatus in 2018 (Dagres, 2022).

2.2.2 Narrative Control

Narrative control is becoming a substantial challenge for the three case studies as EMAs increase in their relevance for news consumption. Valenzuela (2013) outlined a three-step model of mobilization when he noted that social media is related to social movements in three major aspects: information sharing, political expression, and mobilization. While this paper addresses all three, the reliance on EMAs for daily news intake in particular fulfills the aspect of information sharing—a prerequisite of the other two. The regimes are largely relying on two main strategies to counter this: censorship and scaling up of state propaganda.

Online censorship

Censorship occurs largely along the earlier described lines and is justified by various security and media legislation—e.g., the Moroccan press code from 2016, which contains provisions that specifically apply to online media and largely relies on fines (with imprisonment looming if payments fail). All three countries have some sacrilegious topics: In Morocco, these are any criticism of the King or disputing the official opinion on Western Sahara; in Egypt, these are any criticism of Sisi or expressing support for political Islam; and in Iran, any criticism of Ayatollah Khamenei or his

3 The antiterrorism law foresees prison terms of 2–6 years and fines of 10,000–200,000 dirham for culprits of terrorism through offline or online speech (Freedom House, 2021).

predecessor Khomeini—among other things related to the countries' domestic and international alliances.

Censorship on EMAs, however, is much more difficult due to very different content regimes compared to other social media platforms. Therefore, Iran has resorted to blocking. Since the so-called Green Movement in 2009, the theocracy understands social media as a national security threat—similar to Egypt and Morocco since 2011 (Article 19, 2017). The most popular social media sites are blocked, such as Facebook, Twitter, and YouTube (Iran International, 2019). After Telegram in 2018, Signal became the most recent international EMA to be blocked in early 2021—both justified with the need to protect national security (WhatsApp remains unblocked at the time of writing) (Alimardani & Elswah, 2020; Motamedi, 2021). However, our interviewees emphasized another aspect of censorship: self-censorship (Aida, Naomi, Mohammad, Roky). The regime strategies of persecuting people under draconian legislation and making examples of journalists and activists who speak up lead to a widespread understanding of the danger of expressing dissent—including on EMAs, but to a lesser extent: "There is also a reason why Signal was banned—the state knows it gives better protection" (Sarah).

Flooding of state content

In addition to the reactive strategy of censorship, the regimes are also proactive in drafting and spreading state propaganda. EMAs have been integrated into the ecosystem, but traditional media as well as open social media platforms such as Facebook are still prevalent.

In Egypt, a prolific ecosystem has developed composed of public and private stakeholders. Government ministries themselves dedicate resources to the spread of state content and messaging. But they also hire people who support by "handling many bots online" or setting up accounts to flood the internet with state content (Roky). Under Sisi, the regime has been working to amass as much control as possible, including an expansion into the media landscape—not just newspapers and television, but also production companies for film as well as third-party social media marketing firms (Yee, 2022). EMAs factor into this comprehensive propaganda apparatus. It has become common practice for members of the government to do a press release via WhatsApp: "People joke but it's actually quite true that the media landscape is operated out of a WhatsApp group and oftentimes you will see, not just the exact same headline, but the exact same wording of an article in different newspapers" (Stephanie). This can be traced back to high-ranking government members running WhatsApp groups with a number of editors-in-chief of the major news outlets. In addition, the state relies on younger people who act as social media influencers while considering their work a service to the country. One of our interviewees who had been doing this for a few months considered it "a new version of the military service" (Mohammad).[4]

In Iran, computational propaganda is employed to spread messages widely, but state-sponsored troll armies also work to silence dissidents, especially in the vocal diaspora—often with an added gender bias (Article 19, 2021b; Kargar & Rauchfleisch, 2019). In March 2021, a video went viral that seemed to be a tutorial on how to exploit software that inorganically adds likes to social media posts (Dagres, 2022). In Morocco, a plethora of Instagram influencers expressed support for the current prime minister in the weeks leading up to the election (Emad). While it is difficult to identify paid propagandists, the overlaps between politicians who had a successful track record in marketing campaigns and those who are now particularly apt at spreading their political messages is a valuable indicator. The research also found similar dynamics in government-journalist interaction on WhatsApp, albeit less top-down than in Egypt (Ala, Perri). But still, problematic press and antiterrorism laws place high burdens on intermediaries, and social media trolls harass and intimidate people who criticize authorities (Freedom House, 2021a).

4 The use of influencers was also confirmed by people from El Fagr we spoke to. Another type of influencers not covered in this paper but with wide reach are religious leaders such as Imam Mazhar Shaheen in Egypt (El Masry, 2016).

3 CONCLUSION AND POLICY IMPLICATIONS

This research shows how structural social conditions in these countries overshadow the technological potential EMAs hold in terms of their reach and increased significance for information sharing. In other words, the societal fear of the regime's security forces in all three countries, the trauma from the 2013 Rabaa massacre in Egypt, the repeated crackdowns on demonstrators in Iran, and the creeping depoliticization in Morocco stand in the way of the potential EMAs carry for mass mobilization. These insights speak to the need for techno-skepticism in creating social movements and regime challenges, because even if security forces might not have the technical capabilities to access discussions on EMAs, the societal fear keeps many from forming movements. At the same time, EMAs have developed into important means for journalists and main technological facilitators for ad hoc politicization. This also means that the potential ascribed to EMAs can play out very differently in other country contexts, as potential affinity between them and social movement mobilization must be considered in the particular technological, social, and cultural settings (Poell & van Dijck, 2015), or when an additional trigger like regional dynamics are added, such as in 2011.

For **Western policymakers and the international community**, the implications from this research are threefold. *First*, they should try to hold regimes accountable for human rights abuses and punish the harassment of opposition voices. One journalist in Egypt said that he would like to introduce me to other interviewees, but everyone he could think of is in prison. The impunity with which some state forces act and the pushing of boundaries when persecuting activists is related to the level at which world powers, such as the U.S., are willing to overlook the abuses. In practice, a stricter approach would come with opportunities and challenges for the international community. One challenge is the willingness of other authoritarian countries to fill potential gaps created by Western withdrawal when punishing severe human rights abuses by authoritarian governments.

The impunity with which some state forces act and the pushing of boundaries when persecuting activists is related to the level at which world powers, such as the U.S., are willing to overlook the abuses.

For example, Putin has been working to create good relations with the Sisi regime as part of a larger infiltration of Russian influence in the region, including by deploying mercenaries in parts of North and Central Africa, such as Libya or CAR (Yachyshen, 2020). Still, the U.S. and Europe have important influence on the Egyptian and Moroccan governments linked to key issue areas, such as counterterrorism financial/military assistance and the disputed Western Sahara, respectively (Zunes & Mundy, 2022). The main opportunity related to this recommendation for Western policymakers is the potential to instill confidence in local activists, as well as human rights advocates in the diaspora, that democratic governments are willing to draw red lines and stick to them. For instance, individuals and organizations working for democratic change in authoritarian countries could hope that their communication with Western stakeholders would not put them at high risk of detention and/or surveillance if Western policymakers made sure to react to threats to their safety when conducting governmental business. In practice, this means a holistic policy approach, where issue areas are linked to each other.

One way to preemptively inhibit the capabilities of authoritarian regimes is to increase export controls. On the European stage such attempts have been divisive due to the competing interests of not just member states but also different stakeholders within the states. For instance, with regard to the EU's attempts to regulate the export of high-risk surveillance technologies, Germany supported the push for tougher controls on exports of technologies that can be used for both civilian and military purposes, but, for example, Finland, the U.K., and Cyprus were resistant—given their bigger financial interests in that technology sector (Stupp, 2018). Again, the main argument against tighter controls and corresponding decreased export of the mentioned technologies is that other authoritarian governments would try to fill the void, and the strategic relationships of EU members with Egypt, for example, would be damaged.

In addition to export controls, sanctions on individuals who can be tied to cyberattacks targeting institutions of the EU, state or private entities within the individual member states, or other international organizations with offices in and outside the EU are also important measures. For example, the EU undertook such sanctioning for the first time in 2020, targeting Russian, Chinese, and North Korean stakeholders—some of which had carried out an attack on the Organization for the Prohibition of Chemical Weapons (OPCW). These steps are important to signal that those attacks in cyberspace can be considered threatening acts as well.

Generally, however, there is room for improvement to link issue areas and incentivize authoritarian governments with a carrot -and-stick approach (Glowacka et al., 2021). Furthermore, and in line with Western values, it would be appropriate to not only focus on protecting Western societies but also take cyberattacks and online infringements on human rights more seriously when aimed at populations in non-Western countries. Both the U.S. and the EU underperform when it comes to utilizing diplomatic discussions to raise concerns about online censorship, surveillance, or internet shutdowns—including calling out specific countries. In May 2021, a European Parliament report on digital authoritarianism stated that the EU "has not been willing to incur significant costs, in terms of letting trends in digital repression impact its commercial and strategic interests" (Glowacka et al., 2021). Furthermore, the mentioned targeted sanctions have rarely been used in response to human rights violations, nor has the EU taken advantage of its global human rights sanctions regime, which was installed in 2020, as a means to counter digital repression (EU Council, 2020).

Second, while backing by governmental behavior along the outlined lines is important, another aspect of public policy is significant when trying to increase the possibilities of protected information exchange and political communication for local actors: societal knowledge exchange. Though multiple hindrances persist, social movements and civil society organizations are not passive receivers of authoritarian oppression. Instead, they continue to push back and find ways to circumvent censorship. A prerequisite for such action is often the need to protect their own safety. In this regard, institutions such as Meedan are important bridge builders, and others like 7amleh are crucial for building and keeping digital security. The relative safety afforded to organizations in democratic countries (Amnesty International's Security Lab, Citizen Lab, Electronic Frontier Foundation, etc.) can act as leverage for supporting investigations in non-democratic countries and developing technical guidance based on problem assessments with local stakeholders that can then be passed on. One good program is the ad hoc (emergency) grants for digital security and protection measures, of which the EU issued 47 in 2021, that support human rights defenders and activists who are victims of digital repression or seek to combat it (EEAS, 2021). Understanding and supporting (or at least not hindering) this nongovernmental work should be considered in holistic policy assessments. These investments are marginal, however, compared to the scale of increased digital authoritarianism.

Third, Western judicial systems have become an important support mechanism for accountability. This has been significant; for example, in January 2022 a German court in Koblenz found an officer of the Syrian's regime intelligence services guilty of crimes against humanity and sentenced him to life in prison. A more specific criminal case in the cyberspace is when Yahya Assiri, a Saudi human rights activist; Anas Altikriti, founder of the Cordoba Foundation;

and Mohammed Kozbar, vice president of the MAB, declared that they plan to sue the NSO group as well as the governments of Saudi Arabia and the UAE in the U.K., alleging that the two states employed Pegasus spyware when they were in the U.K. (Akkad, 2022). Another case is when Loujain al-Hathloul, a Saudi women's rights defender who was incarcerated and tortured after being arrested in the UAE, filed a case against American employees at DarkMatter for their role in hacking her phone in the U.S. Keeping these legal routes open should be a prerogative for Western policymakers (Schectman & Bing, 2021).

For **researchers**, this paper emphasizes the difficulties of understanding the dynamics of protest mobilization in more closed social media spaces such as EMAs. At the same time, it points out their relevance, as those channels have shown to be limited avenues for free expression in authoritarian states and, furthermore, developed into the main technological facilitators for ad hoc politicization. In addition, journalists, who are often intermediaries for social movements, rely on it. These important contributions to the nucleus of democratic actions are directly linked to encryption. Therefore, upholding E2EE on messaging apps seems crucial. This call for upholding E2EE is at odds with policy attempts in the U.K. or EU that aim to partially unravel encryption under the rationale of child safety or better law enforcement online (EU Commission, 2022). Generally, political leaders orient themselves to legislation introduced in Western countries in order to create higher legitimacy for their repressive legislation. Delving into this aspect further and outlining the repercussions of limiting encryption in Western contexts would be an important contribution to a global debate that needs locally shaped policies. Of course, this includes factoring in other regulations under the EU's Digital Services and Markets Acts, such as easier ways to challenge content-moderation decisions, which is significant as well.

In turn, this drives home a point made for **Western policymakers** earlier—namely, to draw red lines and pursue a value-driven approach. In practice and for the cyberspace, this could mean constructing policy frameworks in tandem with some Middle Eastern countries that would support their digital economy. Within this consultation process, however, the demand to respect their population's rights to privacy and free expression should be conveyed as well. The EU's General Data Protection Regulation (GDPR) was a milestone and one that EU governments could further try to promote internationally as a guiding framework. For example, technology firms that are well-versed in operating under the GDPR could expand into MENA countries and aim to establish their presence/offices in those countries—while supporting local pushes for technological developments, including data localization efforts (Soliman, 2021; Egyptian Ministry of Communications and Information Technology, 2016). Skepticism, however, is well founded; Egypt, for example, put in place a data protection regulation that was heavily inspired by the GDPR and other international standards. However, in practice the law's prohibition of accessing and collecting, processing, transferring, and saving sensitive personal information, without written consent from the individual and approval by the data regulator, is often ignored. Instead, Marwa Fatafta (2020) from Access Now argues that the regulation's main goal is data control rather than protection, as the regime's security is largely unregulated by this law or has other ways to circumvent restrictions, such as placing people on the board of the data regulator (see Lynch, 2022, for a more elaborate discussion).

Finally, **tech companies** should keep in mind the different contexts in which their platforms are used. In Egypt, Iran, and Morocco, these messaging apps have developed into more than free or cheap tools for texting; instead, EMAs have taken on political significance. Therefore, tech companies offering EMAs should consult particularly with journalists in Egypt, Iran, and Morocco to understand how they use the platforms and which platform features could facilitate sharing quality news. On the flipside, EMAs play a role in enhancing disinformation campaigns across the globe, and company representatives would be well advised to draw up mid- to long-term strategies about how to take on responsible policies in different contexts—not just ad hoc ones like those adopted after Russia's invasion of Ukraine (Kraus, 2022).

Most important with regard to EMAs is balancing the protection of civil society activists with [a] platform's exploitation for disinformation purposes.

Most important with regard to EMAs is balancing the protection of civil society activists with the platform's exploitation for disinformation purposes. Platforms would need to invest additional resources not only in quantitatively increased and qualitatively more nuanced content moderation, but also in understanding local contexts and consulting non-Western communities when rolling out new features for their platforms. For example, are increased moderation capabilities for group administrators helpful? Are metadata interventions such as limiting and highlighting message forwarding (still) useful? How can the apps' features be improved to help journalists share information outside the eyes of regime censors? Given the different company structures of EMAs, this would need to be addressed differently. In short, if tech companies are genuinely interested in supporting positive, democratic change around the world, they would need to address their development processes and factor in the Global South much earlier in their product/feature developments. Tech companies should also support local outreach programs explaining different affordances and varying security levels.

Overall, the paper's insights emphasize that social movements and regime challenges are not created by encrypted technologies, because even if security forces might not have the technical capabilities to access discussions on EMAs, the societal fear, uninterest, or skepticism keeps many activists from forming movements (Jeffries, 2013). This points out the contributive, instead of central, nature of technologies to social mobilization: the technical affordances of these apps are not enough to motivate people in authoritarian contexts to form a movement. Therefore, international policymakers should incorporate the outlined deliberations into their policy approaches, which treat the cyberspace as one issue area interlinked with others—in other words, address signs of digital authoritarianism in various ways beyond targeted sanctions or market policies. International organizations such as the UN and its partner organizations like UNESCO have been working to establish frameworks, such as UNESCO's efforts regarding artificial intelligence (2021) or other state-led approaches such as the American Declaration on the Future of the Internet (White House, 2022), which mirrors attempts like the Internet Governance Forum. These are important initiatives emphasizing a human-rights-led approach to the digital world. However, the global trend with regard to internet freedom and security is regressing, so Western policymakers and societies need to understand that they are to expect some economic hits or increased geopolitical competition if they follow through on their ideals in cyberspace (as they should).

REFERENCES

Ali, S. R., & Fahmy, S. (2013). Gatekeeping and citizen journalism: The use of social media during the recent uprisings in Iran, Egypt, and Libya. *Media, War & Conflict, 6*(1), 55-69.

Africa Center for Strategic Studies. (2022, April 26). Mapping Disinformation in Africa. https://africacenter.org/spotlight/mapping-disinformation-in-africa-russia-china/

Akkad, D. (April 19, 2022). UK-based Pegasus targets threaten lawsuits against NSO, UAE and Saudi Arabia. *Middle East Eye.* https://www.middleeasteye.net/news/pegasus-spyware-uk-targets-threatens-lawsuits-nso-uae-saudi-arabia

Amnesty International. (2020a, August 28). Egypt: Joint statement: Veteran human rights defender Bahey el-Din Hassan sentenced to 15-years in prison punished for his critical tweets. https://www.amnesty.org/en/documents/mde12/2951/2020/en/

Amnesty International (2020b, September 25). German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed. https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/

Amnesty International. (2021a, September 16). Egypt: "This will only end when you die": National Security Agency harassment of activists in Egypt. https://www.amnesty.org/en/documents/mde12/4665/2021/en/

Amnesty International. (2021b). In a post-COVID-19 world, "fake news" laws, a new blow to freedom of expression in Algeria and Morocco/Western Sahara. https://www.amnesty.org/en/latest/news/2020/05/in-a-post-covid19-world-fake-news-laws-a-new-blow-to-freedom-of-expression-in-algeria-and-morocco-western-sahara/

Amnesty International. (2022, January 12). Egypt: Authorities must repeal the outrageous NGO law. https://www.amnesty.org/en/documents/mde12/5154/2022/en/

Alimardani, M. & Elswah, M. (2020). Trust, Religion, and Politics: Coronavirus Misinformation in Iran. *SSRN Electronic Journal.*

Article 19. (2017, March 17). Iran: Arrests and intimidation of Telegram administrators and journalists ahead of elections. https://www.article19.org/resources/iran-arrests-and-intimidation-of-telegram-administrators-and-journalists-ahead-of-elections/

Article 19 (2021a, February 19). Iran: Parliament passes law to further choke freedoms and target minorities. https://www.article19.org/resources/iran-parliament-passes-law-to-further-choke-freedoms-and-target-minorities/

Article 19. (2021b, October 19). Online Harassment Against Women Journalists in the Iranian Diaspora. https://www.article19.org/resources/online-harassment-against-women-journalists-in-the-iranian-diaspora/

Article 19. (2022, March 17). Iran: Human rights groups sound alarm against draconian Internet Bill. https://www.article19.org/resources/iran-human-rights-groups-sound-alarm-against-draconian-internet-bill/

Attia, Ashraf M., et al. (2021). The power of social media: a showcase of behavioural change in the 2019 Algerian uprising. *International Journal of Business Forecasting and Marketing Intelligence 1*(1), 70-89.

Bahar, S. (2021, December 13). Iran's water is running dry. Now its water woes are worsening. Atlantic Council. https://www.atlanticcouncil.org/blogs/iransource/irans-water-is-running-dry-now-its-water-woes-are-worsening/

Bhardwaj, D. (2021, June 24). Messaging app Signal not in compliance with new rules, say officials. *Hindustan Times*. https://www.hindustantimes.com/india-news/messaging-application-signal-not-in-compliance-with-new-rules-say-officials-101624508925464.html

Bayat, A., Fathian, M., Moghaddam, N. B., & Saifoddin, A. (2021). The adoption of social messaging apps in Iran: Discourses and challenges. *Information Development 39* (1), 72–85, https://doi.org/10.1177/02666669211022032

Bertelsmann. (2022a). *Index for Political Transformation*. The Transformation Index. https://bti-project.org/en/?&d=D&cb=00000

Bertelsmann. (2022b). Index for Governance Performance. The Transformation Index. https://bti-project.org/en/?&d=G&cb=00000

Bitso, C., Fourie, I., & Bothma, T. (2013). Trends in transition from classical censorship to Internet censorship: selected country overviews. *Innovation 46*, 166-191.

Borshchevskaya, A. L. (2021). Russia's soft power projection in the Middle East. *Military Review,* 32-45.

Buchanan, C. (2015). Revisiting the UNESCO debate on a New World Information and Communication Order: Has the NWICO been achieved by other means? *Telematics and Informatics, 32*(2), 391–39.

Castells, M. (2012). *Networks of Outrage and Hope: Social Movements in the Internet Age.* Polity Press.

Center for Human Rights in Iran (CHRI). (2018, May 22). Iran's Telegram Users Back on the Rise Three Weeks After State Banned the App. https://www.iranhumanrights.org/2018/05/irans-telegram-users-back-on-the-rise-three-weeks-after-state-banned-the-app/

Chu, D. S. (2018). Media use and protest mobilization: A case study of umbrella movement within Hong Kong schools. *Social Media+ Society, 4*(1).

Cohen, T. (2022, June 20). *Morocco used NSO's spyware to snoop on journalist, Amnesty says*. Reuters. https://www.reuters.com/article/us-cyber-nso-group-morocco-idUSKBN23T1PG

Crooms, I. (2018, July 11). Current Moroccan Consumer Boycott is Threatening the Political Status Quo. International Republican Institute. https://www.iri.org/news/current-moroccan-consumer-boycott-is-threatening-the-political-status-quo/

Dagres, H. (2022). *Iranians on Social Media*. Atlantic Council.

Debackere, E. & Akouh, Y. (November 12, 2021). Five Years of Riffian Protests: We See No Difference. *Carnegie Endowment.* https://carnegieendowment.org/sada/85770.

Diamond, L. (2010). Liberation technology. *Journal of Democracy, 21*(3), 69-83.

Diwan, I. (2016). "The Political Effects of Changing Public Opinion in Egypt." In E. Sayre, & T. Yousef (Eds.), *Young Generation Awakening: Economics, Society, and Policy on the Eve of the Arab Spring*. Oxford UP.

Egyptian Ministry of Communications and Information Technology. (2016). Egypt ICT Strategy 2030. https://mcit.gov.eg/en/ICT_Strategy

Einifar, M., & Kosari, M. (2020). How Iranian women express themselves through social media photos: A case study of Instagram. *Journal of Cyberspace Studies*, *4*(1), 1-26.

El Gendy, A. (2022, April 4). When Stories Break Free. *TIMEP.* https://timep.org/commentary/analysis/when-stories-break-free/

El-Khalili, S. (2013). Social media as a government propaganda tool in post-revolutionary Egypt. *First Monday.*

El Masry, M. (2015, August 14). The Rabaa massacre and Egyptian propaganda. *Middle East Eye.* https://www.middleeasteye.net/opinion/rabaa-massacre-and-egyptian-propaganda

El Masry, M. (2016, January 16). Another Arab Spring is coming to Egypt. *Al Sharq Forum*. https://research.sharqforum.org/2016/01/26/another-arab-spring-is-coming-to-egypt/

Enjolras, B., Steen-Johnsen, K., & Wollebaek, D. (2013). Social media and mobilization to offline demonstrations: Transcending participatory divides? *New Media & Society 15*(6), 890-908.

EU Commission. (2022, May). Fighting child sexual abuse: Commission proposes new rules to protect children. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2976

EU Council. (2020, December 7). EU adopts a global human rights sanctions regime [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2020/12/07/eu-adopts-a-global-human-rights-sanctions-regime/

European External Action Service (EEAS). (2021). Report of the EU High Representative for Foreign Affairs and Security Policy: 2021 Annual Report on Human Rights and Democracy in the World. https://www.eeas.europa.eu/sites/default/files/documents/EEAS_annual_Report_HR-2021.pdf

Ezzat, H. (2021). Behavior of fans towards social media influencers in Egypt. *Journal of Communication and Media Research, 13*(1), 62-71.

Fatafta, M. (September 20, 2020). Egypt's new data protection law: data protection or data control? *Access Now.* https://www.accessnow.org/egypts-new-data-protection-law-data-protection-or-data-control/

Farrell, H. (2012). The consequences of the internet for politics. *Annual Review of Political Science, 15*(1), 35-52.

Frampton, M. (2018). *The Muslim Brotherhood and the West: A History of Enmity and Engagement.* Harvard University Press.

Freedom House. (2021a). *Country reports.* https://freedomhouse.org/explore-the-map?type=fotn&year=2021

Freedom House. (2021b). *Freedom of the Net Report: Morocco.* https://freedomhouse.org/country/morocco/freedom-net/2021

Frosina, S. (2021). *Digital Revolution: How Social Media Shaped the 2019 Hong Kong Protests.* ISPI. https://www.ispionline.it/en/publication/digital-revolution-how-social-media-shaped-2019-hong-kong-protests-30756

Gerbaudo, P. (2012) *Tweets and the streets: social media and contemporary activism.* Pluto Press.

Glaser, B.G. (1992) *Basics of Grounded Theory Analysis: Emergence vs. Forcing.* Sociology Press.

Glowacka, D., Youngs, R., Pintea A., & Wolosik, E. (April 2021). *Digital technologies as a means of repression and social control.* European Parliament, DROI Subcommittee. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653636/EXPO_STU(2021)653636_EN.pdf

Gursky, J., Glover, K., Joseff, K., Riedl, M.J., Pinzon, J., Geller, R., & Woolley, S. C. (2020, October 26). *Encrypted propaganda: Political manipulation via encrypted messages apps in the United States, India, and Mexico.* Center for Media Engagement. https://mediaengagement.org/research/encrypted-propaganda

Gursky, J., Riedl, M. J., Joseff, K., & Woolley, S. (2022). Chat Apps and Cascade Logic: A Multi-Platform Perspective on India, Mexico, and the United States. *Social Media+ Society, 8*(2).

Hamidi, M. (2021, January 27). Iranians Continue Protests; Including Retirees' Widespread Rally on January 26. *Iran News*. https://irannewsupdate.com/news/insider/iranians-continue-protests-including-retirees-widespread-rally-on-january-26/

Herbert, M. & Ghoulidi, A. (2019, March 25). *Social media bridges North Africa's divides to facilitate migration.* International Institute for Security Studies (IISS), https://issafrica.org/iss-today/social-media-bridges-north-africas-divides-to-facilitate-migration

Holleis, J, and Knipp, K. (2021, July 22). Egypt: 'Facebook Girl' may be free, but oppression remains rife. Deutsche Welle. https://www.dw.com/en/egypt-facebook-girl-may-be-free-but-oppression-remains-rife/a-58579742

Hussain, M. M. (2014). Digital infrastructure politics and Internet freedom stakeholders after the Arab Spring. *Journal of International Affairs*, 37-56.

Ibahrine, M. (2003.) Towards a national telecommunications strategy in Morocco. *First Monday, (9)*1. https://firstmonday.org/ojs/index.php/fm/article/download/1112/1032#i4

Isfahani, S. (2021, August 9). *Iran Aims to End Online Freedoms 'for Good.'* Slate. https://slate.com/technolo- gy/2021/08/iran-protection-bill-internet-censorship.html

Iran International (2019, August 25). 35 Percent of World's Most Visited Websites Are Blocked in Iran. https://iranintl.com/en/iran/35-percent-world's-most-visited-websites-are-blocked-iran

Iranian Student Polling Agency (ISPA). (2021a). How Citizens Follow the News of the Community; the Authority of Islamic Republic of Iran Broadcasting as the Most Important Source of News Has Decreased in Recent Years. http://ispa.ir/Default/Details/fa/2338/

Iranian Student Polling Agency (ISPA). (2021b). 73.6 Percent of People over the Age of 18 in the Country Currently Use Social Media/WhatsApp Messenger Ranks First. http://ispa.ir/Default/Details/fa/2282.

Jeffries, F. (2013). Mediating fear. *Global Media and Communication*, *9*(1), 37-52.

Kargar, S. & Rauchfleisch, A. (2019). State-Aligned Trolling in Iran and the Double-Edged Affordances of Instagram. *New Media & Society, 21*, 7.

Kermani, H. (2018). Telegramming News: How have Telegram channels transformed journalism in Iran?. *Türkiye İletişim Araştırmaları Dergisi,* (31), 168-187.

Kirchgaessner, S. & Jones, S. (2022, May 3). Over 200 Spanish mobile numbers 'possible targets of Pegasus spyware.' *The Guardian*. https://www.theguardian.com/world/2022/may/03/over-200-spanish-mobile-numbers-possible-targets-pegasus-spyware

Kraus, R. (2022, March 2). *In the Russia-Ukraine information war, encrypted messaging apps provide opportunity and risk.* Mashable. https://mashable.com/article/whatsapp-telegram-russia-ukraine-disinformation

Langlois, G., Elmer, G., McKelvey, F., & Devereaux, Z. (2009). Networked Publics: The Double Articulation of Code and Politics on Facebook. *Canadian Journal of Communication, 34*(3).

Lee, F. et al. (2021) Affordances, movement dynamics, and a decentralized digital communication platform in a networked movement. *Information, Communication & Society* (2021): 1-18.

Lee, F. L., Chen, H. T., & Chan, M. (2017). Social media use and university students' participation in a large-scale protest campaign: The case of Hong Kong's Umbrella Movement. *Telematics and Informatics, 34*(2), 457-69.

Lynch, James. (2022, June 19). *Iron net: Digital repression in the Middle East and North Africa.* European Council on Foreign Relations (ECFR). https://ecfr.eu/publication/iron-net-digital-repression-in-the-middle-east-and-north-africa/

Magdi, A. (2020, October 13). *Protests Still Scare Egypt's Government*. Human Rights Watch. https://www.hrw.org/news/2020/10/13/protests-still-scare-egypts-government#

Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (2018). *HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to operations in 45 countries.* Citizen Lab. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Mandour, M. (2022, March 23). A Homeland Lives Within Us, But We Cannot Live in It: Egyptian Organizing and Activism from Exile. *TIMEP.* https://timep.org/commentary/analysis/a-homeland-lives-within-us-but-we-cannot-live-in-it-egyptian-organizing-and-activism-from-exile/

Masbah, M., Aourraz, R., Idrissi, H., Baumann, A., & Lahrach, T. (2022). *Trust Index 2022: Trust in Public Administration during the Era of Pandemic*. Moroccan Institute for Policy Analysis. https://mipa.institute/9017

Martin, Z., Glover, K., Trauthig, I. K., Whitlock, A., and Woolley, S. (2021, December). *Political talk in private: Encrypted messaging apps in Southeast Asia and Eastern Europe.* Center for Media Engagement. https://mediaengagement.org/research/encrypted-messaging-apps-in-southeast-asia-and-eastern-europe

Motamedi, M. (2021, January 26). Iran Blocks Signal Messaging App after WhatsApp Exodus. *Al Jazeera.* https://www.aljazeera.com/news/2021/1/26/iran-blocks-signal-messaging-app-after-whatsapp-exodus

Moore-Gilbert, K., & Abdul-Nabi, Z. (2021). Authoritarian downgrading, (self)censorship and new media activism after the Arab Spring. *New*

Media & Society, 23(5), 875–893.

Morocco News. (2021, March 12). 84% of Moroccans use WhatsApp in 2021. https://moroccolatestnews.com/84-of-moroccans-use-whatsapp-in-2021/.

Murdoch, S. & Roberts, H.. (2013). Introduction to: Internet Censorship and Control. Available at SSRN: https://ssrn.com/abstract=2268587

Nisbet, E. C., Stoycheff, E., & Pearce, K. E. (2012). Internet use and democratic demands: A multinational, multilevel model of Internet use and citizen attitudes about democracy. *Journal of Communication, 62*(2), 249-265. https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1460-2466.2012.01627.x

Noureldin, O. (2016, February 16). *Egypt orders arrest of Facebook administrator after unfaithful wives comments*. Reuters. https://www.reuters.com/article/us-egypt-unfaithful-controversy-idUSKCN0VP27E

North Africa Post. (2022, March 25). Morocco-COVID-19: State of health emergency extended until 30 April 2022. https://northafricapost.com/56495-morocco-covid-19-state-of-health-emergency-extended-until-30-april-2022.html

Onuch, O. (2014). *Mapping Mass Mobilization. Understanding Revolutionary Moments in Argentina and Ukraine.* Springer.

Oxford Business Group. (January 2017). Investment in Egypt's telecoms network infrastructure boosts revenue. https://oxfordbusinessgroup.com/overview/expanding-opportunity-investment-telecoms-network-infrastructure-boosting-revenues

Poell, T. & van Dijck, J. (2015). Social media and activist communication. In *The Routledge companion to alternative and community media*, Atton, C. (Ed.). Routledge, 527–37.

Reuters. (2020, March 19). *Morocco makes a dozen arrests over coronavirus fake news.* https://www.reuters.com/article/us-health-coronavirus-morocco/morocco-makes-a-dozen-arrests-over-coronavirus-fake-news-idUSKBN2162DI

Schectman, J. & Bing, C. (2021, December 9). *Saudi women's rights activist says phone hack by U.S. contractors led to arrest - lawsuit.* Reuters. https://www.reuters.com/legal/litigation/saudi-womens-rights-activist-says-phone-hack-by-us-contractors-led-arrest-2021-12-09/

Schmidt, A. L. et al. (2017). Anatomy of news consumption on Facebook. *Proceedings of the National Academy of Sciences, 114*(12), 3035-3039.

Similar Web. (2021). *Top Apps Ranking - Most Popular Apps in Egypt.* https://www.similarweb.com/apps/top/google/store-rank/eg/communication/top-free/

Soliman, M. (2021, January 6). *In the Middle East, cyber sovereignty hampers economic diversification.* Middle East Institute. https://www.mei.edu/publications/middle-east-cyber-sovereignty-hampers-economic-diversification

Srinivasan, D. (2019). The antitrust case against Facebook: A monopolist's journey towards pervasive surveillance in spite of consumers' preference for privacy. *Berkeley Business Law Journal, 16*(1). https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/berkbusj16&section=5

Statista. (2021). *Most used social media platforms in Morocco in 3rd quarter 2021.* https://www-statista-com.libdata2015.hilbert.edu/statistics/1243924/leading-social-media-platforms-morocco/

Stupp, C. (2018, June 8). *Nine countries unite against EU export controls on surveillance software.* Euractiv. https://www.euractiv.com/section/cybersecurity/news/nine-countries-unite-against-eu-export-controls-on-surveillance-software

Tech Against Terrorism. (2021). *Terrorist Use of E2EE: State of Play, Misconceptions, and Mitigation Strategies*. https://www.techagainstterrorism.org/wp-content/uploads/2021/09/TAT-Terrorist-use-of-E2EE-and-mitigation-strategies-report-.pdf

The Economist Intelligence Unit. (2008, August 18). Iran: Telecoms and technology background. https://web.archive.org/web/20060813091822/http://www.ebusinessforum.com/index.asp?layout=newdebi&country_id=IR.

Trauthig, I. K. (2021). *Counterterrorism in North Africa: From Police State to Militia Rule and the Quagmire of "CVE."* International Centre for the Study of Radicalisation (ICSR). https://icsr.info/wp-content/uploads/2021/08/ICSR-Report-Counterterrorism-in-North-Africa-From-Police-State-to-Militia-Rule-and-the-Quagmire-of-CVE.pdf

Trauthig, I. K. & Woolley, S. (2022, March). E*scaping the mainstream? Pitfalls and opportunities of encrypted messaging apps and diaspora communities in the U.S.* Center for Media Engagement. https://mediaengagement.org/research/encrypted-messaging-apps-and-diasporas

Tufekci, Z. & Wilson, C. (2012). Social Media and the Decision to Participate in Political Protest: Observations From Tahrir Square. *Journal of Communication, 62,* 363-379.

UNESCO. (2020). *Recommendation on the ethics of artificial intelligence.* https://en.unesco.org/artificial-intelligence/ethics#recommendation

Urman, A., Ho, J.C., & Katz, S. (2020). 'No Central Stage': Telegram-based activity during the 2019 protests in Hong Kong [preprint].

U.S. State Department. (2021, March 30). *2020 Country Reports on Human Rights Practices: Morocco.* https://www.state.gov/reports/2020-country-reports-on-human-rights-practices/morocco/

Valenzuela, S. (2013). Unpacking the use of social media for protest behavior: The roles of information, opinion expression, and activism. *American behavioral scientist, 57*(7), 920-942.

Wagner, B. (2012). Push-button-autocracy in Tunisia: Analysing the role of Internet infrastructure, institutions and international markets in creating a Tunisian censorship regime. *Telecommunications Policy 36*(6), 484-492.

Walker, S. (2020, November 7) 'Nobody can block it': how the Telegram app fuels global protests. *The Guardian.* https://www.theguardian.com/media/2020/nov/07/nobody-can-block-it-how-telegram-app-fuels-global-protest

WhatsApp. (2022). The threat of traceability in Brazil and how it erodes privacy. https://faq.whatsapp.com/general/security-and-privacy/the-threat-of-traceability-in-brazil-and-how-it-erodes-privacy

Weidmann, N. B., & Rød, E. G. (2019) *The Internet and political protest in autocracies.* Oxford Studies in Digital Politics.

White House. (2022, April 28). *A Declaration for the Future of the Internet.* https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf

Wiseman, J. (2020, October 3). Push to pass 'fake news' laws during Covid-19 intensifying global media freedom challenges. *International Press Institute.* https://ipi.media/rush-to-pass-fake-news-laws-during-covid-19-intensifying-global-media-freedom-challenges/

Yachyshen, (2020, November 23). Russia now has a position on Libya: What next? *Foreign Policy Research Institute (FPRI).* https://www.fpri.org/article/2020/11/russia-now-has-a-position-in-libya-what-next/

Yee, V. (2022, May 1). In Egypt's Big Ramadan TV Drama, the President Is the Hero. *New York Times.* https://www.nytimes.com/2022/05/01/world/middleeast/egypt-ramadan-tv-el-sisi.html

Zarhloule, Y. (2020). Framing Nationalism in times of a pandemic: The Case of Morocco. *The COVID-19 Pandemic in the Middle East and North Africa, 55.*

Zeitzoff, T. (2017). How Social Media Is Changing Conflict. *Journal of Conflict Resolution, 61*(9), 1970–1991.

Zimmermann, F., & Kohring, M. (2018). „Fake News" als aktuelle Desinformation. Systematische Bestimmung eines heterogenen Begriffs. *M&K Medien & Kommunikationswissenschaft, 66*(4), 526-541.

Zunes, S., & Mundy, J. (2022). *Western Sahara: War, nationalism, and conflict irresolution.* Syracuse University Press.

Identifying Internet Legislative Trends in Latin America: A Historical Perspective on Internet-Related Bills Across 23 Years

Kimberly Anastácio and Mariana Sanchez-Santos

ABSTRACT:

This paper offers a historical analysis of the patterns of Latin American internet-related bills. We conducted a topic modeling analysis of 520 Brazilian and 57 Chilean bills introduced across 23 years, from the earliest year of available data. We followed the approach of other studies using statistical techniques to map internet regulatory and discursive trends and complemented the results with a close qualitative analysis of the bills' content and historical internet-related events in the region. When policymakers propose internet-related bills, they use language purposefully to advance their intent and reasoning. Our analysis focuses on bills instead of laws, since our main goal is to understand what themes instigate lawmakers and prompt them to attempt to regulate the internet in two countries in the Global South. Our study contributes to internet and platform governance debates on two core issues: What themes motivate lawmakers' responses? How do these responses change over time? Initial results demonstrate that early bills mainly tried to expand internet access and regulate telecommunications in the region, as well as criminalize certain behaviors online. However, recently the focus of lawmakers shifted from bridging the digital divide and controlling users' behavior to regulating the platform economy. This pattern is part of the global policy turn to platforms.

KEYWORDS: Internet regulation, internet policy, Chile, Brazil, bills, topic modeling

1 INTRODUCTION

Policymaking is a communicative process in which legislators make assumptions about what a problem is and how to solve it. When policymakers propose internet-related bills, they use language purposefully to advance their intent and reasoning (Lentz, 2011). This research aims to shed light on what themes instigate lawmakers and prompt them to attempt to regulate the internet. It contributes to internet and platform governance debates by asking: What themes motivate lawmakers' responses? How do these responses change over time?

We focus on two emerging countries from Latin America, Brazil and Chile, and map thematic trends in bills created across 23 years. After conducting a topic modeling and qualitative content analysis on the bills in both countries, we demonstrate that early bills mainly tried to expand internet access and regulate telecommunications in the region, as well as criminalize certain behaviors online. However, recently the

focus of legislators shifted from bridging the digital divide and controlling users' behavior to regulating the platform economy. This pattern is part of the global policy turn to platforms (Keller, 2018; Gillespie, 2018; Gorwa, 2019).

2 INTERNET REGULATION IN EMERGING COUNTRIES

Questions about if and how the internet should be regulated are as old as the internet itself. Historically, there has been an aversion to governmental input on internet-related policies, especially when it comes to large social media platforms and online content services (Napoli & Caplan, 2017). Some assume that internet policy belongs primarily to the private sector, technical experts, or multistakeholder initiatives. However, while recognizing the contentious debates surrounding state and private regulation and control over the internet (DeNardis, 2014), currently most scholars and users alike seem to agree that internet regulation takes place in different forms and at different levels, including through the direct action of national legislators and policymakers (Kerr et al., 2019).

The internet is a product of the input and choices of several corporate, civil society, technical, user, and state initiatives (Mansell, 2012). The internet is a pervasive part of the world in which we live, expanding also to the material objects all around us (DeNardis, 2020). As such, global interest in internet policies is ever more so pushed into the spotlight. Even some private companies themselves, following their own strategies, argue in favor of greater internet regulation and governmental oversight when it comes to issues such as data protection and content moderation (Zuckerberg, 2019).

When the commercial internet arose in the late '90s, the internet appeared to be drifting in the direction of opposing regulatory options amid incipient legislative battles and law enforcement decisions: information anarchy or perfect control (Cohen, 2012). Over time, three broad stories to describe the relationship between the law and the internet were consolidated (Hughes, 2002). The first is a "no-law internet," in which cyberspace is fundamentally inhospitable to traditional law as a mechanism of control. The second is the "internet as a separate jurisdiction," in which cyberspace needs and allows some kind of laws, but its technical characteristics make it resistant to traditional laws, and thus it needs to be its own jurisdiction. The third is internet law as "translation" of traditional legal concepts, recognizing that old and new laws that are applied in the physical world are rendered to the virtual one, too (Hughes, 2002).

Tensions between these three approaches are manifested in internet governance discussions: the administration and development of technologies that keep the internet running, as well as the policy formulation around and regulation of these technologies (DeNardis, 2020). They are also at the core of platform governance issues: the governance layers that structure the interactions between key parties in a platform society dominated by the global corporations operating Facebook, WhatsApp, YouTube, and many other online services, and that address both the political effects of digital platforms and the challenge of regulating the platform themselves (Gillespie, 2017; Gorwa, 2019; Keller, 2018; Gillespie, 2018).

Recent scholarship on internet governance has suggested a focus on the role of the state in internet regulation. For instance, while addressing internet governance as an arena where power is contested among diverse state and non-state actors, be they at the local, national, regional, or global scales, Haggart et al. (2021) disregard a dichotomy between anarchy and perfect control, libertarianism and authoritarianism. The authors assume that internet regulation occurs across the lines between state and non-state actors, and national legislators are a key part of this process.

When it comes to platform governance, especially due to growing regulations about content moderation that arose from the debates on disinformation and political polarization online, the media field is facing a "policy turn" or "regulatory turn" (Flew, 2019; Flew et al., 2019). In many democratic countries, the public is increasingly looking to their national governments to solve internet-related

problems, such as misinformation, freedom of speech, and net neutrality, through regulatory solutions (Keller, 2018; Kerr et al., 2019; Flew et al., 2019; Cammaerts & Mansell, 2020).

To better understand and situate these current trends demanding internet regulation, we conduct a historical analysis of internet-related proposed legislation in two Latin American countries: Brazil and Chile. Scholarship surrounding internet policy has long tried to address if the internet is regulable, who should regulate it, what issues would fall under such regulation, and how regulation should occur (Litan, 2001; Lessig, 2006; Goldsmith & Wu, 2006; Zittrain, 2008). Nevertheless, most answers to these questions have been modeled after and produced in developed countries (Carr, 2015; Miao et al., 2021). The inclusion of the perspectives and knowledge of emerging countries, such as Brazil and Chile, is key to both challenging and strengthening arguments around internet regulation. A comparison between countries is also adequate. Brazil and Chile have high levels of internet penetration (76% and 82%, respectively; Statista, 2022) and both countries have introduced regulatory frameworks for the internet constantly over the past 20 years. The complex and global nature of internet regulation pushes us to consider how different national legal systems try to solve similar problems, since regional differences must be overcome to create convergence in legal systems around the world (Hughes, 2002).

Additionally, whenever one proposes media and internet policies, there is the challenge of regulating a range of technologies and business practices that are ever dynamic in nature (Claffy & Clark, 2014). To account for the evolving nature of technologies, we take a longitudinal approach that allows us to identify trends in internet regulation over time. We turn to internet-related bills proposed by lawmakers in Brazil and Chile to identify what themes prompt their regulatory intent and how lawmakers understand the problems they are trying to solve.

Both Chile and Brazil have presidential systems with an executive branch, a legislative branch, and a judicial branch. In this article, we focus on the legislative power. Both countries have a similar process to create laws. Many bills are filed every year, though the majority of them will not become law. Still, bills in Brazil and Chile have the clear intent to propose regulatory changes, even if some of them are proposed to signal commitments to, for example, interest groups and voters. In this analysis, we focus on the themes pushing the legislators' intent to regulate the internet, and not on what has successfully become written law.

2.1 INTERNET POLICYMAKING AS A COMMUNICATIVE PROCESS

Words matter when we analyze regulatory texts and policies (Lentz, 2011). Those who build regulation use language intentionally to design, architect, and construct policy in certain ways instead of others. As Napoli and Caplan (2017) argue, "the specific terms employed in the discourse and documents that shape and reflect policy decisions have profound consequences, and thus are employed strategically" (p.13). Words serve a strategic purpose, often in order to determine the contours of an issue. Thus, one can see regulation and policymaking as communicative processes (Popiel, 2020). Policy discourses and regulatory texts not only express strategic legislators' goals; they also foster specific ideological projects and are a site for contestation and conflict (Popiel, 2020; Lentz, 2011).

Those who build regulation use language intentionally to design, architect, and construct policy in certain ways instead of others.

The study of law should be perceived as a cultural practice as it relates to how law constructs and is constructed by its everyday context (Ewick & Silbey, 1998; Gash & Harding, 2018). As explained by Ewick & Silbey (1998), legality embodies the diversity of the situations in which it emerges and is not sustained only by formal institutions such as the constitution, statutes, and courts. Legality is sustained because it relies on the commonplace of everyday life. Policymaking, then, is a communicative process where the "construction of legal meanings, actions, practices and institutions" (Ewick & Silbey, 1998, p. 18) is a feature of social relations. Internet policy is a field of struggle in which a constellation of actors contends over meaning-making around the issues on the table (Pohle et al., 2016). We analyze how one such actor, national legislators, creates meaning around internet regulation through the internet-related bills they propose.

3 METHODS

This paper employs topic modeling in the text of internet-related bills, following the approach of other studies that rely on statistical techniques to map internet regulatory and discursive trends (Shahin, 2019; Miao et al., 2021). The increase in computational power and storage has accelerated the potential to use text-mining techniques across a range of scholarly fields (Cogburn, 2020, p. 190; Murakami et al., 2017; Shahin, 2019). Topic modeling is one such technique and can "be conceptualized as a way of describing what a text is about" (Murakami et al., 2017, p. 244). It takes the unstructured text and transforms it into a structured numerical format, making it ready for treatment with standard data-mining techniques (Cogburn, 2020, p. 190).

Probabilistic topic modeling automatically identifies the main themes (topics) that pervade a large and otherwise unstructured collection of documents that comprise a corpus of words (Blei, 2012). We use the Latent Dirichlet Allocation (LDA) approach to topic modeling (Blei et al., 2003). With LDA, it is possible to identify a series of keywords that have a statistically high probability of co-occurrence. Together, these keywords form a topic that represents a meaningful theme. It is also possible to identify the proportion of use of each topic in the documents (Shahin, 2019, p. 6).

In this paper, the corpus comprises 520 Brazilian and 57 Chilean internet-related bills. We chose Brazil and Chile because they both have the highest internet penetration in South America and have historically been active in trying to regulate the internet. Brazil is also home to the Marco Civil da Internet, a law celebrated as one of the most innovative internet policies in the world, which also influences legislation in the region (Moncau & Arguelhes, 2020). Chile was the first country in the world to introduce a bill that later became a law on the principle of Net Neutrality in 2010.

We collected all bills from each country's House of Representatives' website, searching for bills that contain the word "internet" in their titles and/or summaries—a short piece of the text where lawmakers outline the main purpose and objectives of their bills. Chile's House of Representatives (Honorable Cámara de Diputadas y Diputados de Chile) has a website that contains a section called "Legislative Activity" (www.camara.cl) where one can search for bills. We searched for the term "internet" from 1998 to 2021. In total, we found 57 bills that contain the term "internet" in their titles. For Brazil, we extracted the information from the House of Representatives (Câmara dos Deputados) website (www.camara.leg.br) for the same period, representing the earliest year of data available in a readable format. We also searched for the same query ("internet").[1]

Some internet-related bills may not explicitly mention the word "internet" in the title but still refer to internet-related problems and issues. However, our focus in this paper is solely on the pieces of proposed legislation that clearly label themselves as internet-related bills and that mention the term explicitly. Additionally, we collected proposed

1 The main difference between the data collection for both countries is that for Brazil we employed a web-scraping tool that collected all the bills and converted them to .txt files. Thirty-four bills that contained the word "internet" in their titles were not available in a .txt format (e.g., bills published on the website as a photo of a printed document) and were not included in this analysis.

TABLE 1. Number of internet-related bills by year (Brazil, N = 520 / Chile, N = 57)

YEAR	BRAZIL	CHILE
1998	2	-
1999	1	1
2000	0	-
2001	0	-
2002	4	3
2003	15	-
2004	9	-
2005	7	2
2006	6	1
2007	9	10
2008	12	6
2009	13	-
2010	17	5
2011	33	2
2012	18	3
2013	18	3
2014	8	1
2015	51	3
2016	51	3
2017	36	-
2018	24	3
2019	62	-
2020	68	4
2021	56	7

legislation introduced only in the House of Representatives in order to level the experiences of countries with bicameral congresses that may have different expectations toward the duties of representatives and senators. Moreover, we collected only bills, which are documents that, in both countries, have legislative intent. We did not consider position and opinion papers, as well as requests for public hearings and administrative decrees. Such bills have a similar layout composed of two parts. In one part, the lawmakers introduce the provision proposed. In the other part, they offer a justification for the importance of their proposed legislation. We considered both the provision and justification for our analysis.

The bills were converted into .txt files readable by RStudio, and we ran our analysis using the "topicmodels" R package. Preprocessing included lowercasing, tokenization, and removal of numbers, punctuation, and stop words commonly used in Portuguese and Spanish (e.g., the, it, is). We also removed some words commonly used in bills irrespective of the theme or context of the bill. Such words include "bill," "law," and "representative," all terms that do not contribute to the content analysis of the topics.

Our dataset includes bills regardless of whether they became law through approval by the House of Representatives, were removed by their authors, or were rejected by the representatives. Since our interest is in identifying what themes prompt lawmakers to try to regulate the internet, and how they justify their reasons for doing so, we focus on proposed legislation despite its success or failure in the House of Representatives.

For the qualitative analysis, we complemented the topic modeling with an in-depth content analysis of the bills, trying to find "plausible relationships among concepts and sets of concepts" and create theory from the constant comparison of observations (Babbie, 2010, p. 390). We engaged with the bills in several readings in order to identify themes and their relationships to each other.

Based on this close reading, we determined the overarching themes for each topic established by the text-mining analysis. While reading the bills and trying to match their content with the topic modeling results, we followed four principles for grounded theory: (1) think comparatively; (2) obtain multiple viewpoints; (3) periodically step back

and remember that the "data don't lie" and (4) maintain an attitude of skepticism, regarding observations as provisional (Glaser & Strauss, 1967).

4 RESULTS

In our topic modeling, the number of "topics" identified in the corpus is specified by the researcher, who can choose a greater or lesser degree of granularity in the topics (Murakami et al., 2017, p. 245). Multiple iterations of topic modeling in which we tested different numbers of topics were done, until a model with four topics emerged as the most meaningful and relevant one for each country. Tables 3 and 5 in the Appendix contain examples of the bills and justifications used by the lawmakers on each topic. In this model, the keywords associated with each topic are coherent, which indicates that the topics are not just statistically but also semantically probable (Shahin, 2019).

Four broad topics help explain how regulatory discourse changes over time in Brazil (Table 2 and Figure 1) and four other topics in Chile (Table 4 and Figure 2). Bills in each of the years analyzed are not limited to the topics described in this study. There can be outliers and other themes not covered by the model we used and, each year, bills are not limited to the topic with the highest percentage. Still, the topics described below adequately summarize regulatory trends over the years. The percentage of each topic by year demonstrates that, in comparison with other years, one had the highest probability of sharing certain words and themes among the bills of that same year.

4.1 BRAZIL

For Brazil, four broad topics emerged from our analysis: access to information, platforms and institutions, digital inclusion, and regulating behavior.

4.1.1 Access to Information

Topic 1 represented bills primarily concerned with access to information: the users' potential to obtain content online. As seen in Table 3, this topic was most prominent in the earlier years included in the database (1998–1999, 2005, 2009–2011, and 2014). Several bills determined the removal of any content related to violence, nudity, pornography, or child exposure published on the internet (e.g., Bill 360/2011). Others established that the public sector should make available content relevant to public policy and political issues on governmental websites (e.g., Bill 4576/1998 determines that all public administration should publish reports on tax collection on governmental websites; Bill 6872/2010 determines that the government should make the criminal records of all candidates in a given election year available online). Some bills argue in favor of the removal of access to information online. For example, they try to establish a "right to be forgotten," a right to having certain types of personal information removed from the internet (e.g., Bill 7881/2014).

Regarding the legislators' rationale for proposing bills that fall under such a topic, it is remarkable that they demonstrated curiosity and uncertainty about the possibilities of the internet in their earliest bills. For example, one representative wrote that "as the global network becomes the fastest growing means of communication in the world, becoming popular among regular computer users, we imagine that it can be an efficient instrument in the dissemination of government data" (Bill 4576/1998). Legislators justify their bills on access to information by mentioning the affordances of the internet, including its global nature and fast-paced transmission of information (e.g., Bill 7881/2014).

4.1.2 Platforms and Institutions

Topic 2 primarily encompasses bills that turn to social media platforms and internet companies themselves as the focus of regulation. This topic has been most prominent in the latest years (2017, 2020, and 2021), after the establishment of a key internet law in the country, the Brazilian Civil Rights Framework for the Internet (Marco Civil), in 2014 and during the discussion about the Brazilian General Data Protection Law, approved in 2020. Both laws establish the rights of users in light of the duties of internet platforms. Following such a trend, bills that fall under Topic 2 alter the Marco Civil to strengthen certain policies such as, for example, altering content moderation practices and establishing harsh notice and takedown provisions for hate speech online.

Additionally, some bills turn to internet providers and argue against data caps, a bandwidth restriction. What is constant in bills under such a topic is a focus on the companies, instead of users, as the central point for legislation.

Legislators justify their propositions based on what has already been established by the Marco Civil and considering new events. For example, one representative proposed a bill to impose fines on any company that uses users' data without their consent and justified that:

> The recent Facebook and Cambridge Analytica case demonstrated the need to establish stricter regulations for Internet companies. … leading us to present a bill to curb practices by companies that behave unscrupulously and that are extremely harmful not only to democracy, but also potentially to all aspects of life in society. (Bill 344/2019)

4.1.3 Digital Inclusion

Topic 3 relates to bills mostly concerned with digital inclusion initiatives. The topic appeared with greater relevance in 2015, 2018, and 2020, and concerns mostly bills regarding universal internet access in the country (e.g., Bill 10730/2018). It is noticeable that the topic predominated in 2020, since many bills proposed that year tried to ensure internet access to the Brazilian population during the COVID-19 pandemic. For example, some bills determined free internet access to students doing remote learning (e.g., Bill 3477/2020) or prohibited the termination of internet services due to late payment during the pandemic (Bill 1422/2020).

Many bills proposed [in 2020] tried to ensure internet access to the Brazilian population during the COVID-19 pandemic.

Legislators justify the need for digital inclusion by appealing to the benefits of the internet to society. For example, one legislator stated that "the internet gives citizens a voice" (Bill 185/2015). Another stated that, due to the COVID-19 pandemic, internet access is essential so that citizens have a dignified life and that "at this time of serious insecurity, it is necessary to guarantee the low-income population sufficient tools to respect the health measures adopted by the government," including continuous internet access (Bill 1422/2020).

4.1.4 Regulating Behavior

Topic 4 figured in the greatest number of years (1999–2019). It has to do with users' behavior online and attempts to hold users accountable for content and actions on the internet regarding a broad range of issues. For instance, bills try to criminalize certain abusive behaviors online (e.g., Bill 6127/2002 penalizes the publication of pedophilia content). Others criminalize intellectual property infringements (e.g., Bill 5361/2009). Some are narrow in their focus, for example, prohibiting the online sale of animals to prevent animal exploitation (Bill 858/2019).

Legislators try to adapt laws to the virtual environment and/or try to create new criminal offenses based on the internet. The rationale behind most of the bills trying to regulate users' behavior is summarized by the following justification:

> The internet is a technology that has become indispensable in modern life. However, as with all new technologies, it can also be used for inappropriate purposes … It is evident the need to establish a legal framework to create the foundations for a stable and safe virtual environment where citizens, companies, and governments can interact without being vulnerable and exposed to cybercrime. (Bill 3175/2012)

4.2 CHILE

The four broad topics for Chile include two that are similar to those in Brazil—regulating behavior and access and connectivity—and two other topics—user rights and consumer rights.

4.2.1 User Rights

Topic 1 encompasses issues around users' rights on the internet. As observed in Figure 2 (see Appendix), this topic was most prominent in 1999, 2010, 2016, and 2020. When the early commercial internet arose, there were many legal debates about the rights that people online should or should not have (Lessig, 2006), and legislators in Chile also engaged in such discussions. Bills about users' rights in the country, for instance, tried to regulate net neutrality. For example, as observed in Table 5 (see Appendix), Bill 10999-15 establishes "that only through a court order, the access provider may deny the service of internet content."

This topic was also prominent in 2020 due to the COVID-19 pandemic. As with the Brazilian case, bills established that internet providers should secure free internet to vulnerable students at the beginning of the pandemic. The rationale behind this was that users should have the *right* to access the internet during times of calamity and, as one legislator put it, it was demanded by society, especially "in response to the demand raised by mayors" (Bill 13422-15).

4.2.2 Regulating Behavior

Topic 2, regulating behavior, concerns bills that established guidelines for how users should act online. This topic was prominent in 2008, 2014, and 2015. In comparison with Topic 1, bills that fall under such a topic mentioned social media platforms more. Some bills, for example, try to regulate the buying and selling of medicines and to prevent fraud, identity theft, and practices linked to bullying and violence through social media.

One of the bills proposes that "whoever knowingly films, exhibits or distributes through the internet, material that contains discriminatory conduct, corporal or psychological punishment and intimidation, will be sanctioned with fines of 50 UTM (salary) for tax benefit and community work" (Bill 5896-07). Another example imposes sanctions on identity theft. The legislator justified the criminalization of such a practice online, referring to the argument that the "internet is a platform where forms of human relationships are developed that cannot be left out of the legal system. They must be governed by rules or norms that guarantee not only good functioning but that the fundamental rights of the people are respected" (Bill 9700-07). The rationale for such bills is one that recognizes the importance of ensuring that the virtual environment is subject to the same laws that exist offline.

4.2.3 Access and Connectivity

Topic 3 deals with issues around access and connectivity. We observed this topic for the years 2002, 2005, and 2021. The topic was most prominent in Chile at the beginning of the century and after the COVID-19 pandemic. Bills that fall under this topic try to ensure internet connectivity in the country, e.g., Bill 14586-07 argues that it is the responsibility of "the State to promote and facilitate access to the internet and digital connectivity under conditions of equality, throughout the territory." Bills like this one refer to things happening in the international setting to justify their need. For example, one legislator based his bill on international guidelines proposed by the United Nations, explaining that "in 2016 the Council of Human Rights of the United Nations approved a resolution [that] urges States to 'facilitate and expand access to the internet and requests all States to do everything possible to close the multiple forms of the digital divide.'"

4.2.4 Consumer Rights

Finally, Topic 4 relates to words such as "provider," "service," and "consumer" that represent a shift from people seen as users (Topic 1) to people seen as consumers. Topic 4 was prominent in 2006, 2007, 2012, and 2018, years of significant developments in Chile's digital economy (UNCTAD, 2019). The words used in the examples presented in Table 4 show the change from "user" to "consumer." One of the bills determines a "Consumer protection law, establishing the obligation to publish guaranteed minimum speed in internet access" (Bill 4671-03). The bill suggests that internet providers must indicate in their advertising the speed of the plan they're offering. The rationale behind this bill and other ones that fall under such a topic is primarily an economic one. The legislator justified Bill 4671-03, for example, stating that "harmful effects can be produced in the competition of Internet Providers and prevent the improvement of a competitive and transparent market." Another example

of this topic is a bill that establishes a filter for internet access for minors (Bill 5262-19). The legislator differentiates between minors and internet *consumers*, which would be those older than 18 years old.

5 DISCUSSION AND LIMITATIONS

This study's main goal is to shed light on what themes instigate lawmakers and prompt them to attempt to regulate the internet. It is a historical analysis of bills and the legislators' rationale for regulating the online world. We aimed to understand from a cultural perspective the main motivations for how legislators make meaning when trying to regulate the internet.

Remarkably, legislators in both countries are also pushing for bills that situate internet legislation in light of economic perspectives, trying to regulate and hold accountable internet companies, especially social media platforms.

Both Brazil and Chile share a topic focusing on the regulation of behavior online. Legislators from both countries recognize that the internet has become indispensable in modern life but that it can also be used for undesirable purposes. Thus, they tend to try to criminalize some postures online, offering guidelines for users' conduct and sanctions. Both countries also share topics about digital inclusion and access to information. Topics 1 (access to information) and 3 (digital inclusion) for Brazil and Topic 3 for Chile (access and connectivity) deal with the perception of legislators in these emerging countries about the importance of ensuring that all citizens have access to the internet and to information online. Remarkably, legislators in both countries are also pushing for bills that situate internet legislation in light of economic perspectives, trying to regulate and hold accountable internet companies, especially social media platforms—Topics 1 (users' rights) and 4 (consumer rights) for Chile and Topic 2 (platforms and institutions) for Brazil.

Litan (2001) suggests that lawmakers should not act prematurely when it comes to internet regulation but act pragmatically and with humility to make constant corrections, because the internet "twists and turns" and the policy issues it evokes cannot be predicted in advance (Litan, 2001, p. 1085). The computational method that we employed for this study allows us to see what the "twists and turns" of proposed legislation were. Answering how the bills' themes evolve over time, we highlighted the occurrence of a trend toward internet platforms. Attempts to regulate users' behavior and control what can or cannot be done on the internet were very prominent in the Brazilian case throughout the years (Topic 4, regulating behavior). They were also present in Chile (Topic 2, regulating behavior). Measures to tackle the digital divide and ensure access to information were also present throughout the years. Still, recently, both in Brazil and Chile we found the emergence of a topic focusing more on the digital economy, centered on internet platforms.

Van Dijck (2021) echoes other scholars in highlighting that the current global communication and information system is dominated by internet companies based mainly in the United States and urges European legislators to act as agents of change and propose regulations to reshape platform governance. We demonstrate that such endeavors have long been present in the intent of legislators, at least in two Latin American countries, Chile and Brazil. In light of this finding, we believe we should pay closer attention to

regional initiatives from South America, instead of the usual focus on the Global North, as a locus for internet regulation.

This study focused only on bills of law. While bills are adequate to identify trends in the regulatory intent of lawmakers, future studies should analyze what bills actually become law over the years to understand what eventually reaches consensus among legislators. Such an analysis would follow Pohle et al.'s (2016) suggestion to focus on which regulatory discourses become institutionalized and, thus, produce and change the institutional structure of the communication policy field (Pohle et al., 2016). Comparisons across different regions, including countries from the Global North and South, are also desirable.

6 POLICY RECOMMENDATIONS

The media, communications, and internet governance fields face a "regulatory turn" (Flew et al., 2019). Lawmakers, users, and internet companies themselves are turning to the law to make sense of the public implications of technology. Understanding the past and present regulatory trends, and what motivates legislators, is a fundamental step to shape future internet policy, especially considering the perspectives of emerging countries. We recommend:

1. *Increase access to and quality of the data available on the House of Representatives' websites or similar institutions.*

   This recommendation implies two things:
   a. It is a best practice for legislative institutions to keep track of the bills they produce. Such historical datasets should be made freely available to the public on the internet, as in the Brazilian and Chilean cases. It should be easy to find and collect internet-related bills over time.
   b. Bills should be made available in appropriate formats. Documents in image format—e.g., .jpeg—are not always easily read by text-mining approaches. Formats like .txt, .pdf, or HTML are preferable as a good practice regarding the range of possibilities of usage of bills' data.

Data availability and quality allow for the type of exploration conducted in this study and are vital for cross-country historical analysis.

2. *Increase collaboration between legislators from different countries around internet regulation.*

The Brazilian and Chilean regulatory trends are similar over time, although the countries have different histories, economies, and internet governance institutions. Spaces for the exchange of opinions between lawmakers could prove useful to strengthen regional internet regulation. Sharing experiences about how legislators from different countries, especially those sharing common characteristics, perceive a problem related to the internet and then propose regulatory solutions could lead to better proposals.

REFERENCES

Babbie, E. (2010). *The practice of social research* (13th ed. International). Wadsworth.

Blei, D. M. (2012). Probabilistic topic models. *Communications of the ACM, 55*(4), 77-84.

Blei, D. M., Ng, A. Y., & Jordan, M. I. (2003). Latent dirichlet allocation. *The Journal of Machine Learning Research, 3*, 993-1022.

Carr, M. (2015). Power plays in global internet governance. *Millennium*, 43(2), 640-659.

Cammaerts, B., & Mansell, R. (2020). Digital platform policy and regulation: Toward a radical democratic turn. *International Journal of Communication, 14*, 20.

Claffy, K. C., & Clark, D. (2014). Platform models for sustainable Internet regulation. *Journal of Information Policy, 4*(1), 463-488.

Cogburn, D. (2020). Big Data Analytics and Text Mining in Internet Governance Research: Computational Analysis of Transcripts from 12 Years of the Internet Governance Forum. In: L. DeNardis, D. Cogburn, N.S. Levinson, & F. Musiani (Eds.), *Researching internet governance: Methods, frameworks, futures.* MIT Press.

Cohen, J. E. (2012). *Configuring the networked self: Law, code, and the play of everyday practice.* Yale University Press.

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

DeNardis, L. (2020). *The internet in everything*. Yale University Press.

Ewick, P. & Silbey, S. (1998). *The Common Place of the Law: Stories from Everyday Life*. Chicago University Press.

Flew, T. (2019). The platformized Internet: Issues for Internet law and policy. *Journal of Internet Law, 22*(11), 3-16.

Flew, T., Martin, F., & Suzor, N. (2019). Internet regulation as media policy: Rethinking the question of digital communication platform governance. *Journal of Digital Media & Policy, 10*(1), 33-50.

Gash, A., & Harding, R. (2018). #MeToo? Legal Discourse and Everyday Responses to Sexual Violence. *Laws*, 7(2):21. https://doi.org/10.3390/laws7020021

Glaser, B. G. & Strauss, A. L. (1967). *The Discovery of Grounded Theory. Strategies for Qualitative Research*. Aldine.

Gillespie, T. (2017). Governance of and by platforms. In J. Burgess, A. Marwick, & T. Poell (Eds.). *The SAGE handbook of social media*. Sage, pp. 254-278.

Gillespie, T. (2018). Regulation of and by platforms. In J. Burgess, A. Marwick, & T. Poell (Eds.), *The SAGE handbook of social media* (pp. 254–278). London: SAGE.

Goldsmith, J. & Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World*. Oxford University Press.

Gorwa, R. (2019). What is platform governance?. *Information, Communication & Society, 22*(6), 854-871.

Haggart, B., Tusikov, N., & Scholte, J. A. (Eds.). (2021). *Power and Authority in Internet Governance: Return of the State?*. Routledge.

Hughes, J. (2002). The Internet and the persistence of law. *BCL Rev., 44,* 359.

Keller, D. (2018). *Internet platforms: Observations on speech, danger, and money.* Hoover Institution's Aegis Paper Series, No. 1807.

Kerr, A., Musiani, F., & Pohle, J. (2019). Communication and internet policy: A critical rights-based history and future. *Internet Policy Review, 8*(1), 1–16. https://doi.org/10.14763/2019.1.1395

Lentz, R. G. (2011). *Regulation as Linguistic Engineering. The Handbook of Global Media and Communication Policy*, 432–448.

Lessig, L. (2006). *Code 2.0*. Basic Books.

Litan, R. E. (2001). Law and Policy in the Age of the Internet. *Duke Law Journal, 50*(4), 1045. doi:10.2307/1373102

Mansell, R. (2012). *Imagining the Internet: Communication, innovation, and governance.* Oxford University Press.

Miao, W., Jiang, M., & Pang, Y. (2021). Historicizing Internet Regulation in China: A Meta-Analysis of Chinese Internet Policies (1994–2017). *International Journal of Communication, 15*, 24.

Moncau, L. F. M., & Arguelhes, D. W. (2020). Marco Civil da Internet and Digital Constitutionalism. *The Oxford Handbook of Intermediary Liability Online*. Oxford University Press.

Mu**rakami, A., Hunston, S., Thompson, P., & Vajn, D.** (2017). 'What is this corpus about?' Using topic modelling to explore a specialized corpus. *Corpora, 12*(2), 243–277. doi:10.3366/cor.2017.0118

Napoli, P., & Caplan, R. (2017). Why media companies insist they're not media companies, why they're wrong, and why it matters. *First Monday, 22*(5). https://doi.org/10.5210/fm.v22i5.7051

Pohle, J. & Hösl, M. & Kniep, R. (2016). Analyzing internet policy as a field of struggle. *Internet Policy Review, 5*(3). https://doi.org/10.14763/2016.3.412

Popiel, P. (2020). Let's Talk about Regulation: The Influence of the Revolving Door and Partisanship on FCC Regulatory Discourses. *Journal of Broadcasting and Electronic Media, 64*(2), 341–364. https://doi.org/10.1080/08838151.2020.1757367

Shahin, S. (2019). Facing up to Facebook: how digital activism, independent regulation, and mass media foiled a neoliberal threat to net neutrality. *Information Communication and Society, 22*(1), 1–17.

Statista. (2022). *Internet users as share of the total population in countries in Latin America and the Caribbean as of January 2022.* Retrieved June 22, 2022 from https://www.statista.com/statistics/726145/latin-america-internet-penetration-countries/

UNCTAD. (2019). *Digital Economy Report 2019.* Retrieved May 1, 2022, from https://unctad.org/system/files/official-document/der2019_en.pdf

Van Dijck, J. (2021). Seeing the forest for the trees: Visualizing platformization and its governance. *New Media & Society, 23*(9), 2801-2819.

Zittrain, J. (2008). *The future of the internet--and how to stop it*. Yale University Press.

Zuckerberg, M. (2019, March 30). The Internet needs new rules. Let's start in these four areas. *The Washington Post.* https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html

APPENDIX

TABLE 2. List of terms per topic (Brazil)

TOPIC 1 ACCESS TO INFORMATION	**TOPIC 2** PLATFORMS & INSTITUTIONS	**TOPIC 3** DIGITAL INCLUSION	**TOPIC 4** REGULATING BEHAVIOR
feder	conteúdo	serviço	serviço
dia	serviço	conteúdo	acesso
município	usuário	forma	meio
união	assinatura	rede	consumidor
dado	rede	usuário	usuário
estado	acesso	acesso	rede
serviço	forma	provedor	nacion
conta	br	pessoa	dado
recurso	aplicaçõ	público	público
pública	direito	dado	informaçõ
único	pessoa	ponto	direito
homepag	provedor	meio	empresa
administração	meio	sociai	telecomunicaçõ
público	público	direito	provedor
outra	sociai	informaçõ	sítio
informaçõ	dep	nacion	brasi
deverão	camara	pública	pessoa
contrato	dado	aplicação	crime
tribun	nacion	caso	brasil
publicação	leg	conta	publicação

Source: Author

FIGURE 1. Distribution of topics per year (Brazil)
Source: Author

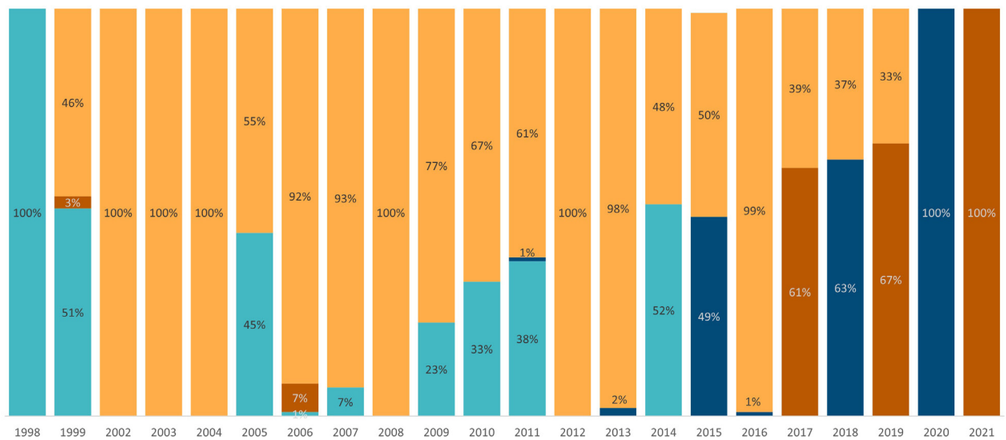


TABLE 3. Examples per topic (Brazil)

TOPIC	BILL SUMMARY	JUSTIFICATION BY THE LEGISLATOR (EXCERPT)
Topic 1 Access to Information	Establishes the creation of a homepage on the internet, by the Court of Auditors, for the dissemination of public data and information. Bill 4576/1998	"As the global network becomes the fastest growing means of communication in the world, becoming popular among regular computer users, we imagine that it can be an efficient instrument in the dissemination of government data."
	Establishes the mandatory dissemination of photographs of missing children and adolescents by internet access providers. Bill 1647/1999	"The internet is a powerful instrument, including because of its international nature: people from other countries will be able to see the information and expose the presence of children and adolescents abroad, because they have been kidnapped or illegally given up for adoption."
Topic 2 Platforms and Institutions	Prohibits internet operators from imposing data limits on fixed broadband. Bill 6944/2017	"Brazilians were surprised by the decision of fixed broadband internet providers to implement a limit to establish limits on data traffic to consumers. This measure offends the population's right to access the internet and, ultimately, harms society's full exercise of citizenship."
	Amends the Marco Civil to create obligations for internet application providers to moderate hate speech. Bill 3700/2021	"Although we know that many of these attitudes can be considered crimes, it is necessary to create a financial incentive for digital platforms to implement a rapid and adequate moderation of this harmful content, removing it. What we aim with this bill is to make it clear that internet platforms, so-called application providers, can become responsible for third-party hate speech on their platforms, if they are not diligent in deleting this content."
Topic 3 Digital Inclusion	Guarantees access to the internet for educational purposes for students and teachers of public schools. Bill 3477/2020	"The real digital barrier is found in internet access. The cost of data plans in the prepaid system is high and the volume of data offered is insufficient for students to execute tasks and for attending remote classes. Internet access systems via public Wi-Fi sports exist, but there is no guarantee that they are provided where the students' homes are located. In this context, we offer this initiative, which ensures a free data package intended for students of the public school system."
	Adds items to the Constitution to ensure universal access to the internet as a fundamental right of citizens. Bill 185/2015	"It is an undeniable fact that the internet has revolutionized the ways of living in society, eliminating physical and temporal barriers, horizontalizing communication and democratizing access to information. The complexity of the contemporary world involves all its sectors. ... Access to the internet today is fundamental for the social, cultural, intellectual, educational, professional, and economic development of any nation."
Topic 4 Regulating behavior	Establishes the crime of disseminating information, messages, or images related to pedophilia or sexual abuse of children or adolescents on the internet, or on other networks intended for public access. Bill 6127/2002	"There are, of course, technical difficulties in the characterization and investigation of this crime. In addition, given the global nature of the internet, a website abroad can be accessed in the country, which makes this content available to our society but, at the same time, makes it impossible to punish the person responsible. This, however, should not prevent the typification of the crime and the establishment of the penalty."
	Creates civil penalties for downloading or sharing electronic files on the internet that contain artistic or technical works protected by intellectual property rights, without authorization from the legitimate owners of the works. Bill 5361/2009	"I consider that it is extremely urgent, especially so that the development of a national culture is not put at risk, that effective measures are adopted to combat digital piracy, a practice that Brazil, unfortunately, is one of the leaders."

TABLE 4. List of terms per topic (Chile)

TOPIC 1 USER RIGHTS	**TOPIC 2** REGULATING BEHAVIOR	**TOPIC 3** ACCESS & CONNECTIVITY	**TOPIC 4** CONSUMER RIGHTS
servicio	travé	dato	servicio
dato	consumidor	servicio	acceso
derecho	bien	electrónico	usuario
acceso	producto	acceso	travé
proveedor	persona	derecho	consumidor
persona	penal	información	información
red	rede	correo	derecho
contenido	social	persona	siguient
protección	venta	ser	contenido
usuario	código	empresa	proveedor
forma	medio	medio	forma
información	inciso	mensaj	velocidad
caso	servicio	usuario	establec
empresa	delito	market	menor
telecomunicacion	información	direccion	part
ser	ser	voluntaria	telecomunicacion
así	siguient	tarjeta	red
bien	mismo	uso	niño
si	anterior	así	persona
social	red	caso	general

Source: Author

FIGURE 2. Distribution of topics per year (Chile)
Source: Author

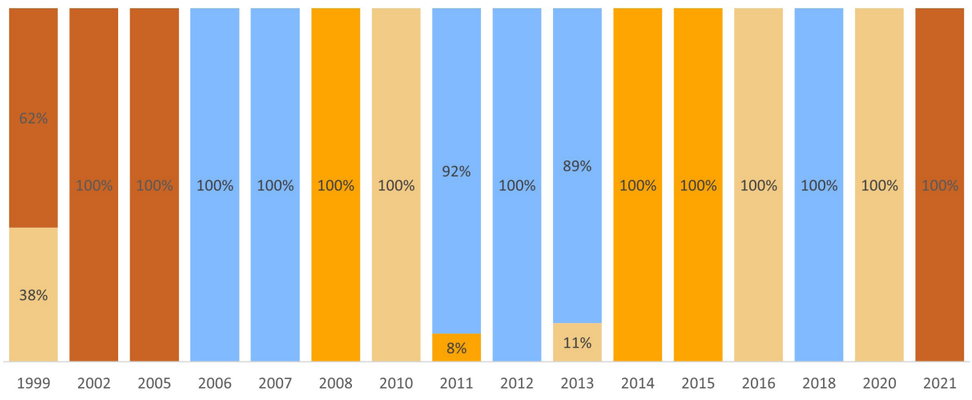


TABLE 5. Examples per topic (Chile)

TOPIC	BILL SUMMARY	JUSTIFICATION BY THE LEGISLATOR (EXCERPT)
Topic 1 User Rights	Modifies Law No. 18,168, on General Telecommunications, regarding the principle of net neutrality. On Net Neutrality Bill No. 10999-15	"Chile was the first country in the world to legislate to guarantee respect for the principle of net neutrality. Based on this guiding idea, companies that provide internet access cannot carry out network management activities to block or discriminate traffic from a content provider. It was an innovative idea in the world of public telecommunications policies, and gave our country great recognition in the international circuit, serving as an example for countries like the Netherlands, Brazil and the United States itself, who subsequently adopted similar measures."
	Modifies Law No. 18,168, General Telecommunications, to establish the obligation of provider companies to deliver free internet to vulnerable students in case of suspension of classes due to the declaration of health emergency. Bill No. 13422-15	"On March 15 of this year, due to the spread of Covid-19 cases in our country, he announced the suspension of classes in kindergartens, municipal, subsidized and private schools for two weeks. This is in response to the demand raised by the mayors and the prohibition of public events with more than 200 people that from that day began to rule in our country."
	Introduces sanctions to "happy slapping," which consists of recording violent acts and then uploading them to the internet. Bill No. 5896-07	People are fully aware of what they are doing, that is why they record it and upload it to the internet, as they seek fame."
Topic 2 Regulating Behavior	Amends the criminal code, with the purpose of punishing identity theft carried out through the internet and social networks, causing damage to third parties. Bill No. 9700-07	"[Every year"'Happy slapping,' is what the English call it. But there is nothing funny about brutal attacks filmed by cell phone or otherwise. The violent acts are beginning in schools where the strongest hit the weakest, filming the events and sending the video clips to their friends or posting them on the internet.] there are more and more complaints of usurpation or identity theft that are made through the internet and social networks, we refer to those made through emails, Facebook, twitter or others. In our country, during the year 2012 these increased by 14% and during 2013 by 49.4%, according to Cybercrime."
Topic 3 Access and Connectivity	Constitutional reform that ensures digital connectivity and access to equal internet to all the inhabitants of the nation. Bill No. 14586-07	"On June 27, 2016, the Council of Human Rights of the United Nations approved a resolution for the "promotion, protection and enjoyment of the human rights on the internet. In that resolution, the Council urges States to 'facilitate and expand access to the internet and requests all States to do everything possible to close the multiple forms of the digital divide.'"
	Amends various legal bodies to ensure student connectivity and internet access as an essential tool in the right to education. Bill No. 14579-04	"The access to technologies and their benefits are not equal, given the differences in access between different population groups. The latter is precisely called the 'Digital Divide.'"

TOPIC	BILL SUMMARY	JUSTIFICATION BY THE LEGISLATOR (EXCERPT)
Topic 4 Consumer Rights	Amends consumer protection law, establishing the obligation to publish guaranteed minimum speed in internet access. Bill No. 4671-03	"Today there is no standard, complete and up-to-date that establishes quality indicators for the internet Access Service provided in our country. Due to the lack of service quality indicators, harmful effects can be produced in the competition of internet Providers and prevent the improvement of a competitive and transparent market, which tends to improve the quality of the internet service offered today."
	Establishes the obligation to use filters for access by minors to commercial establishments that provide internet services. Bill No. 5262-19	"The use of the internet constitutes a valuable educational tool, but at the same time, with inappropriate use, it is a threat to a particularly vulnerable sector of the population; they are minors. This bill aims to legislate in a matter in which the dignity of children and young people is constantly being carried out."

Tackling Misinformation in Emerging Economies and the Global South: Exploring Approaches for the Indian Context

Jhalak Kakkar[1]

ABSTRACT:

While the challenge of misinformation is not new, certain factors in the digital age have heightened its negative impacts on society. In particular, the designs of internet platforms—their algorithms and business models—have enabled the rapid spread of misinformation. Various countries have adopted diverse approaches to tackle this challenge, ranging from speech regulation to self-regulation. However, these approaches have limitations in a Global South or Indian context. Additionally, these approaches do not address the underlying factors that enable the viral spread of misinformation. As India rethinks its Information Technology Act, it must focus on building in regulatory mechanisms around platform transparency and accountability to enable regulators, researchers, and other key stakeholders to effectively understand internet platforms' system of information flows, design elements that enable misinformation virality, and business models. Based on an understanding gained from platforms' enhanced disclosures, greater public awareness can be built around these issues and regulatory frameworks can be designed to ensure greater platform transparency and incentivize a shift in business models away from overreliance on targeted behavioral advertising.

KEYWORDS: Misinformation, Global South, internet platforms, algorithms, transparency, accountability

1 INTRODUCTION

Over the last few decades, we have seen an increasing reliance on internet platforms such as social media platforms, messaging applications, and search engines as modes of communication and news and information sharing. These developments have brought many benefits for society, including the expansion of the scope of the public sphere (Çela, 2015)—an essential factor for the flourishing of a democratic society.

However, while these internet platforms have made the public sphere more inclusive and representative of diverse perspectives, they have also given rise to significant challenges. These challenges include implications for users' fundamental freedoms, particularly for members of marginalized and vulnerable communities, as well as the democratic foundations of our society. One of the key challenges impacting users and democratic discourse is that of the spread of misinformation[2] via these internet platforms.

Historically, the free flow of speech and information has been vulnerable to misinformation or information that may be false, inaccurate, manipulated, or unverified (Turcilo & Obrenovic, 2022). Certain factors in the digital age have exacerbated the flow of misinformation and its negative implications for our society (Ireton et al., 2018). In particular, the design of these internet platforms—their algorithms and business models—have enabled the viral sharing of digital news and content, enabling the rapid spread of misinformation. In the Global South, along with the spread of misinformation on social media platforms such as Facebook and Twitter, misinformation is prevalent on end-to-end encrypted messaging platforms such as WhatsApp. However, for the purposes of this paper, we are focused on the flow of misinformation on social media platforms such as Facebook and Twitter and not on messaging platforms such as WhatsApp.

This spread of misinformation has negative implications for the public sphere. A healthy "public sphere" enables the inclusive and representative discussion of social, economic, and political issues, the formulation of public opinion, and access to credible information (Habermas, 1962). Misinformation corrodes this public sphere and has various negative implications for a society, such as its impact on social cohesion, political polarization, electoral integrity, public health, and trust in democratic institutions.

These implications are heightened in emerging economies/ Global South[3] contexts that deal with low levels of users' digital and media literacy, limited resources for content fact-checking, internet platforms' differential allocation of resources to content moderation in emerging economies compared to developed economies, and often low regulatory capacity of the State to design effective regulation and hold internet platforms accountable. In this paper, we outline regulatory approaches to tackling misinformation, ranging from speech regulation to self-regulation to intermediary liability, and briefly engage with their limitations. We conclude by exploring the approach of platform and algorithmic transparency and whether these could be foundational regulatory mechanisms to aid Global South countries build upon and develop effective approaches to tackle misinformation.

2 REGULATORY APPROACHES TO MISINFORMATION

As emerging economies grapple with how to tackle the challenge of misinformation and its negative impacts on both individuals and our democratic societies, it is useful to look at the various regulatory approaches evolving across the globe. Global South nations should carefully consider lessons from across the globe on what regulatory approaches to adopt, if any, to address the challenges of misinformation.

2.1 LEGAL PROSCRIPTION OF FALSE CONTENT

Countries such as Singapore and Germany have adopted legislation such as the Protection from Online Falsehoods and Manipulation Act (2019) and the Network Enforcement Law (2017), respectively, that prohibit online misinformation. This approach has faced severe criticism by civil society as enabling censorship by the State and violating users' freedom of speech and expression (Human Rights Watch, 2018, 2019).

Lessons from India and across the globe indicate that

1 I am grateful to the National Law University Delhi for supporting the work we do at the Centre for Communication Governance and Dr. Daniel Mathew for his guidance; to my colleagues Shashank Mohan, Aishwarya Giridhar, Joanne D'Cunha, Vasudev Devdasan, Arpitha Desia, and Srishti Joshi for the many discussions I have had with them on these issues and the research input and perspectives they have shared; and to Vasudev Devdasan for coming through as my final reader for the piece.

2 In this paper, misinformation refers to "false or inaccurate information that is deliberately created and is intentionally or unintentionally propagated" (Wu et al., 2019).

3 In this paper, while "Global South" is used in its more traditional sense, readers are urged keep in mind that many of these arguments can be applied to an expansive definition of Global South, to include "countless Souths," including marginalized, disenfranchised, and poor populations in the West. See Arun (2019).

speech laws that impose a legal proscription of false content could have a chilling effect on free speech and undermine the essence of a free and open internet. For instance, in India there have been challenges around the misuse of a legislative provision that regulated online speech; it prohibited the dissemination of false information to cause annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will (Section 66A of the Information Technology Act). In fact, despite this provision being struck down by the India Supreme Court as unconstitutional, there are instances of its continued use by government authorities and the police (Bahri, 2018). Given this experience, careful thought must be given to adopting a speech-based regulation approach to the challenge of misinformation.

2.2 SELF-REGULATION BY PLATFORMS

The European Union (EU) has used a self-regulatory approach with online platforms operating in the EU with the adoption of a self-regulatory code—the Code of Practice on Disinformation ("EU Code")—in 2018 (European Commission, 2018). This approach to tackling misinformation enables internet platforms to regulate themselves and determine key performance indicators, encourages disclosure, and ensures implementation of collectively agreed-upon rules. However, it has not been effective in reducing misinformation. In its first assessment in 2020, the European Commission highlighted various limitations of the EU Code including its self-regulatory nature, the lack of uniformity in implementation, and the need for enforcement and redress mechanisms (European Commission, 2020).

Experience suggests that Global South countries are less able to command the attention of platforms and consequently an approach of self-regulation by platforms is unlikely to lead to the desired level of compliance. Additionally, given the EU's limited success in ensuring implementation of a self-regulatory approach by platforms and the relatively limited regulatory capacity of the State in Global South countries, along with those countries' limited ability to engage with internet platforms and hold them accountable, such an approach may have limited efficacy in enabling Global South countries to tackle the challenges around misinformation.

2.2 CO-REGULATORY APPROACH

Over the last few years, the EU has worked toward developing a co-regulatory approach and has recently adopted the Digital Services Act (Proposal 2020/0361) and Digital Markets Act (Proposal 2020/0374) (European Parliament, 2020a, 2020b). These regulations seek to address the illegal content and manipulative activities that negatively impact users, particularly vulnerable users. It will be interesting to see how this approach evolves, its effectiveness in addressing these challenges, and the lessons that could be translated into the Indian context where a co-regulation approach is not as prevalent.

2.3 INTERMEDIARY LIABILITY

In the Indian context, we are seeing the development of regulation that seeks to use intermediary liability as a mechanism to tackle misinformation.

2.3.1 Current Indian Legislative Framework

In India, though there is no law that specifically targets online misinformation, pre-internet laws such as the Indian Penal Code contain provisions that could be used in the context of misinformation.[4] Additionally, provisions under the Information Technology Act (IT Act) empower the government to block content on the internet and rely on intermediary liability to provide safe harbor to internet platforms for hosting illegal third-party content, as long as they comply with provisions of the IT Act and observe their due diligence obligations (Information Technology Act, 2000). Hence, intermediaries' observance of due diligence obligations and their compliance with the Indian Intermediary Guidelines 2021 (Information Technology Rules, 2021) form a prerequisite for platforms to avail of safe harbor in India and consequently provide us context on the

4 These include sections of the 1860 Indian Penal Code: sedition (s. 124A), obscenity (s. 292), defamation (s. 499), intentional insult with the intent to cause breach of peace (s. 504), statements having potential to result in public mischief (s. 505), hurting religious sentiments (s. 295A), and promoting enmity between different groups and doing acts prejudicial to the maintenance of harmony (s. 153A).

enforcement and implications of the Guidelines.

It is noteworthy that the Indian Intermediary Guidelines 2021 contain a provision requiring significant social media intermediaries[5] that provide messaging services to enable the identification of the first originator of information, as required by various court orders or government authorities (Rule 4(2), Rules 2021). As per the Guidelines, these orders can be made for the purpose of the prevention, detection, investigation, prosecution, or punishment of offences related to state and national security or offences related to rape, sexually explicit material, or child sexual abuse material. The context of these guidelines seems to indicate that the government sees this provision as a mechanism to tackle challenges around fake news and misinformation (Press Trust of India, 2019; MeitY, 2021; Reuters, 2018).

Social media intermediaries and technology experts have argued that complying with orders requiring them to identify the first originator of the information will require them to break end-to-end encryption of these platforms (Agarwal, 2021a, 2021b), despite the government's assertion that it did not intend to undermine the technology (Aryan, 2021; MeitY, 2021). The government has not undertaken any steps to ensure the traceability of the first originator of information (Alawadhi, 2021). These provisions are being challenged in appeals courts in India (Rajan, 2021), and careful thought has to be given to the implications of such a regulatory mechanism to tackle misinformation and the chilling impact this could have on users' freedom of speech and expression.

Recently, the government proposed a regulation that would require platforms to make reasonable efforts to remove content flagged as fake or false by certain government bodies (MeitY, 2023). These government bodies include the Press Information Bureau (PIB) and any Union Government department. While this may not require the proactive removal of content declared as false, once informed of the "fake" or "false" nature by such a government department, internet platforms would be required to remove such content. A failure to comply with this would result in the loss of safe harbor for the platform. This proposal to empower government bodies to determine content that is fake or false raises serious concerns around the restriction of citizens' freedom of speech and expression. Article 19(2) of the Indian Constitution allows the government to restrict speech on certain grounds, such as public order, the security of India, or the prevention of defamation. The Supreme Court in 2015 stated that government orders to remove content must be in consonance with the grounds articulated in Article 19(2). Here it is relevant to note that the Indian Constitution does not allow the government to restrict speech on the grounds of speech being fake or false. Additionally, the proposed regulation also does not adhere to processes and safeguards set up under Section 69A of the IT Act around the takedown of content by the government. The government has sought public comments on this proposal, and it remains to be seen how this regulation progresses.

2.3.2 Recent Amendments to the Indian Intermediary Guidelines

Until recently as per the legislative framework, platforms needed to ensure that their Terms of Service (ToS) prohibit users from uploading or sharing various categories of content (unlawful content) such as content that is harmful to children; infringes any trademark, patent, or copyright; is defamatory; threatens public order or the security of India; is obscene; or violates any Indian law (Rule 3(1)(b), Rules 2021). In particular, from the perspective of misinformation, one of the unlawful content categories covered is content that is "patently false or misleading in nature but may reasonably be perceived as a fact"; platforms must prohibit such content in their ToS (Rule 3(1)(b), Rules 2021).

Large social media platforms work toward removing these categories of content as part of their voluntary content moderation activities. The Intermediary Guidelines require platforms to inform their users, at least once a year, that noncompliance with the platform's ToS may result in the removal of such categories of content or the termination of the user's access to the platform (Rule 3(1)(c), Rules 2021). Platforms are legally obligated to remove such content when they receive "actual knowledge" of this unlawful content on their network—interpreted in the Supreme Court

5 Significant social media intermediaries are those intermediaries with more than five million registered users in India.

case Shreya Singhal to be a court order or a government order (§ 79(3), IT Act; Rule 3(1)(c), Rules 2021; Shreya Singhal v. UOI, 2015).

However, recently the Ministry of Electronics and Information Technology (MeitY) amended the Intermediary Guidelines via the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022, that place further obligations on intermediaries in the context of unlawful content (MeitY, 2022). The amended rules require intermediaries to not only include prohibitions against unlawful content in their ToS, but also to "cause the user" not to upload or share such content and to "ensure compliance" with the platform's ToS (Rules 3(1)(a)-3(1)(b), Amendment Rules).

Hence, a literal interpretation of this language may suggest that the amendments change the platforms' legal obligation for content such as misinformation from an obligation to include prohibitions against such content in their ToS, to a requirement to prevent users from uploading such content onto their platforms. This may result in a strict liability standard for platforms, since the hosting of unlawful content by a platform would be a violation of its obligation to prevent users from uploading such content, leading to a violation of the Intermediary Guidelines and hence a loss of safe harbor. This could trigger platforms to be overcautious and take down wide categories of content, resulting in excessive censorship of content on these platforms and negative implications for users' speech rights. This may be particularly challenging in the context of misinformation; given the difficulty of ascertaining "falsehoods" online, the propensity for lawful speech to be accidentally taken down is far greater than for other types of unlawful content, such as gambling or child sexual abuse material.

However, such an interpretation of the 2022 amendments would conflict with the safe harbor provision of the Information Technology Act, Section 79, and other provisions of the Intermediary Guidelines. Section 79(1) of the IT Act explicitly provides intermediaries immunity for hosting unlawful content. This platform immunity would be rendered meaningless under a literal interpretation of the 2022 amendments to the Intermediary Guidelines. Section 79(1) of the IT Act constitutes primary legislation; the 2022 amendments amend the Intermediary Guidelines, which is delegated legislation. Thus, the 2022 amendments cannot override the legislative framework enumerated in Section 79. However, the adoption of these amendments seems to point to the fact that platforms will undertake the regulation of content such as misinformation, under the rubric of intermediary liability.

It is relevant in this discussion to distinguish between the content of the regulation (the category of speech that is prohibited) and the enforcement (who determines what is prohibited or legal speech). In the recent amendments, government-formulated speech rules are enforced by platforms. This can be contrasted with the approach in the U.S., where both the speech rules and enforcement is done by the platforms. There may be variance between the definitions of various platforms on what constitutes "misinformation"; however, they may be more nuanced than a government standard of "patently false."

An intermediary liability-based approach to misinformation may have various limitations. It raises fundamental questions about who are intermediaries, what we see as their obligations, and what protections are available to them—all of this has significant implications for freedom of speech and expression online. Another challenge with such an approach may be that intermediary liability primarily relies on enforcement through civil and criminal lawsuits. However, in the context of Global South countries, where lawsuits are expensive and the court systems are typically overburdened and consequently slow, there is a question of how effective such an approach can be. As jurisprudence develops around the liability of platforms as publishers/distributors for their recommender systems, it may raise further challenges around the applicability of intermediary liability as a tool.

An intermediary liability-based approach to misinformation … raises fundamental questions about who intermediaries are, what we see as their obligations, and what protections are available to them.

As discussed above, approaches that rely on content and speech regulation or intermediary liability, as well as approaches that rely on platform self-regulation, have various limitations in ensuring effective regulation of these platforms and user access. As Global South countries grapple with the challenge of misinformation and the negative impacts it has on user rights and the democratic moorings of our societies, it is important to explore approaches that go beyond digital literacy and fact-checking to more fundamental solutions that address the complex systems of information flows online and the internet platform design elements that facilitate the propagation of misinformation. Below we explore one such alternate approach: platform and algorithmic transparency and platform accountability, threads of which are emerging in the recently adopted EU regulations. As the Indian government reportedly drafts a fresh Information Technology Act (Mathi, 2022) to tackle the significant challenges posed by internet platforms, it is a prime opportunity to explore such an approach and integrate it into the legislative framework the government is currently designing.

3 AN ALTERNATE APPROACH TO PLATFORM REGULATION: Platform Transparency and Accountability

The primary tool of platform regulation is centered around intermediary liability and content regulation. However, while this is required, these regulations do not tackle the underlying causes of platform harms and may in fact lead to unintended impacts. These include incentivizing platforms to overcensor content to limit liability. There is increasing recognition that many of the harms arising from internet platforms originate from their design and the targeted behavioral advertising business models they are based on. Algorithms play a role in content moderation, content recommendation, and targeted advertising on internet platforms. Consequently, regulatory measures that ignore these aspects of platforms are likely to have limited effectiveness or result in unintended consequences, such as restrictions on information flows and the right to speech. Consequently, as countries like India redesign their legislative frameworks that, like the IT Act, primarily regulate social media platforms, it is important for the government, civil society, industry, and academic stakeholders to have meaningful conversations around platform design, transparency, and business models.

Through the use of algorithms and big data, internet platform users are profiled and targeted (Privacy International, 2017). The design of internet platforms amplifies misinformation via "microtargeting"—directing tailored content toward users to help content go viral (Jones et al., 2016; Vaidhyanathan, 2018); algorithms that encourage polarization of user opinions; fake accounts or bots that amplify content reach; and a business model propelled by targeted behavioral advertising (Ranking Digital Rights, 2020; Nadler et al., 2018).

Algorithms are designed to enhance user engagement through likes, shares, retweets, and comments. Literature indicates that the algorithmic design of internet platforms, including Google, Facebook, and Twitter, is structured to prioritize increased user engagement over delivery

of credible content (George, 2018). This links with the propagation of filter bubbles and polarization, as well as increased flows of misinformation. Relatedly, it is argued that information-related harms depend more on the scale of dissemination than on the content itself. The scale of dissemination is driven by the metrics prioritized by algorithms—content likely to enhance user engagement is prioritized, creating a "snowball" effect (Barnhart, 2021). Those driving misinformation leverage these platform design features to enable the proliferation of misinformation (Horwitz, 2021a). The Oxford Internet Institute at the University of Oxford refers to this as "computational propaganda"—the use of algorithms, automation, and human curation to purposefully distribute misinformation over social media platforms (Woolley & Howard, 2018).

Algorithms are not neutral; they prioritize specific values and consequently shape the information sphere.

Additionally, the platform's primary source of revenue is driven by targeted advertising. There is concern that this also leads to the prioritization of user engagement over other metrics (Horwitz, 2021b) and consequently drives the algorithms' prioritization of sensational content such as misinformation. Hence, it is key to highlight that algorithms are not neutral; they prioritize specific values and consequently shape the information sphere. In 2019, an internal Facebook memo disclosed by whistleblower Frances Haugen highlighted that "the mechanics of our platform are not neutral," and platform design and features, including virality, recommendations, and content optimization for engagement, are key to enabling misinformation to flourish on the platform (Isaac, 2021). Research suggests that this may be true for other internet platforms, including Twitter and TikTok (Little, 2021). Regulatory frameworks based on liability may not always effectively address challenges such as misinformation, since it may often require these platforms to make decisions on content removal that do not necessarily align with their business models. Consequently, effectively addressing the challenges and harms posed by platforms would require us to closely examine the underlying design and business models of these platforms. As India redesigns its IT Act, it is important that legislators and the government explore mechanisms beyond speech regulation, self-regulation, and intermediary liability, and instead focus on exploring mechanisms for regulating the underlying causes of the proliferation of harmful content such as misinformation. We are seeing an increased global interest in transparency regimes, with the UK, New Zealand, and Brazil designing such regimes and the EU recently adopting relevant provisions. These regimes include (1) information disclosed to the public, regulators, and auditors; (2) researcher access to data mechanisms; (3) risk assessments and disclosure of those assessments; (4) transparency by regulators to the public; (5) transparency of processes such as complaints and appeals mechanisms; (6) transparency in platform terms and conditions; and (7) comprehensibility and accessibility (particular languages or formats). Three key ideas pertinent to this discussion are explored below.

3.1 INFORMATION DISCLOSURE AND PLATFORM TRANSPARENCY

One of the key challenges in proposing effective regulatory interventions addressing platforms' underlying features is the significant information asymmetry between platforms and other stakeholders, and the limited information available in the public domain on the functioning of platforms, their business models, and their systems of algorithmic decision-making. Additionally, there is very limited disclosure or any independent oversight or scrutiny for inherent bias or harm of these algorithms (Crain & Nadler, 2019; Neyazi, 2019). While certain technology companies have voluntarily disclosed information relating to their algorithms, pledging to be more transparent (Mayor, 2019), many do not disclose information. Understanding the design and functioning of platforms is a foundational

step in shaping effective regulation, as well as reimagining alternate models of platform design. It is also a key step in building public awareness around the functioning of these platforms and their impact on our societies, and in helping build consensus on how platforms need to evolve.

There are various sources of information on platforms, including voluntary disclosures by platforms such as periodic transparency reports, third-party sources such as leaked information, public filings, and mandatory disclosures by platforms such as disclosures to government (Keller & Leerssen, 2019). However, the detail and kind of information available in these sources is varied, challenging to compare, or lacking adequate context to derive meaningful insights. For instance, often reporting and disclosure are in formats that are not useful, or the information categories are often not comparable across companies, with either different or unclear definitions of what constitutes each information category.

For India to effectively design regulatory solutions to tackle the challenges posed by platforms, there is a need for enhanced platform transparency and meaningful information disclosure on algorithmic functioning (discussed in the next subsection). Transparency and access to information for a cross section of stakeholders are necessary to frame effective accountability measures that potentially reduce harms such as misinformation (Llansó, 2020). The Indian Intermediary Guidelines 2021 introduced a requirement that significant social media intermediaries publish monthly transparency reports regarding their content moderation activities. While this is a step in the right direction, an assessment of the information published by the intermediaries points to fragmented and limited information. Additionally, currently this transparency is focused on disclosing information around content moderation practices, and it may be useful to explore other aspects of platform transparency such as advertising or algorithmic functioning. Consequently, there is a need for Indian authorities to articulate categories and formats of information that may be useful to enhance platform transparency and disclosures around algorithmic functioning.

Multistakeholder consultations need to be undertaken in India not only to identify categories of information relevant in the Indian context that platforms should be required to disclose, but also to start to develop broad consensus on formats this information can be disclosed in to facilitate comparative analysis across platforms.

3.2 ALGORITHMIC TRANSPARENCY

Relevant information that the redesigned IT Act could require platforms to disclose with respect to algorithmic transparency includes how the algorithms work and when they are used (Diakopoulos & Koliska, 2016), how these algorithms are developed (Diakopoulos & Koliska, 2016), the logic of the model or overall design (Ananny & Crawford, 2018), and the factors relevant to the functioning of the algorithm, such as data points. The question that arises is to which categories of stakeholders—ranging from government, regulators, academics, civil society, technical experts, general public, and industry—such disclosures of information should be made and to what extent information should be shared with each category. Platform companies' concerns around proprietary information and confidential business strategies need to be considered when designing these disclosure mechanisms. A graded disclosure system can be adopted that provides detailed disclosure to regulators and the basic levels of disclosure to the general public. Detailed analysis of other regulatory sectors, such as the patent system and drug assessment mechanisms for pharmaceutical companies, could provide insights on how to design an effective system.

Globally, we are seeing developments toward enhanced algorithmic transparency. For instance, the EU General Data Protection Regulation (GDPR) (2016) requires that organizations be able to explain the logic behind their algorithmic decisions that have a significant impact on individuals (Article 13-15, GDPR, 2016). The EU's recently adopted Digital Service Act requires platforms to provide transparency into their recommender algorithms (Vincent, 2022). In the United States, various legislative proposals like the Banning Surveillance Advertising Act (2022), the Algorithmic Justice and Online Platform Transparency Act (2021), the Nudging Users to Drive Good Experiences on

Social Media Act 2022), and the Algorithmic Accountability Act (2022) have been introduced to tackle the issues of algorithmic decision-making and create transparency and oversight measures of automated systems.

While the recently proposed Indian Digital Personal Data Protection Bill 2022 requires platforms to undertake data protection impact assessments in certain circumstances, it does not protect against the specific harms arising from automated profiling and decision-making. Given that the Indian government is reportedly working on an updated Information Technology Act, within this new regulation for internet platforms there is a need to expand the nature of impact assessments to include audits and transparency requirements for platforms' algorithms. Regulation could require that internet platforms be subject to independent audits and enhanced transparency requirements. Public consultations should be done across the globe on who would be the most appropriate stakeholder to conduct such audits—regulators, researchers, approved third-party auditors, or a body composed of various stakeholders. Perhaps quarterly human rights audits based on a jointly chosen committee of experts with representation from regulators, civil society, and technical experts may be the way forward.

To incentivize increased transparency and accountability from internet platforms, the legislation can potentially develop a public scoring or rating system that indicates the level of compliance with algorithmic transparency and disclosure norms. Such transparency will provide the public with access to information such as how internet platforms collect and use user data, how they profile and target users, and how their algorithms determine what content should target specific users.

3.3 RESEARCHER ACCESS TO INFORMATION

A complementary element crucial to understanding information flows on these platforms and equipping stakeholders with capacity to design and propose effective regulatory solutions to address harms would be enabling researcher access to information on platforms. Some platforms, such as Facebook, Twitter, and ShareChat, offer researchers different levels of access to data on information flows. For example, in the past, more research has been done on misinformation on Twitter, in part due to the platform's expensive but open access to data, with YouTube, Google Search, and Facebook offering decreasing levels of data to external researchers (Benkler et al., 2018). Such access has been more limited in the Global South. It would be useful for the redesigned IT Act to potentially delineate a requirement for platforms to enable researcher access to information on their platforms.

One key aspect to keep in mind is which would be the appropriate person or body to make an assessment of the credibility and relevance of a researcher request for access—the platforms themselves, a government body or regulator, or an independent panel of experts and academics? Each of these approaches has limitations. Platform incentives may not always align with the transparency and information sought in a particular researcher access request; hence, it may not be appropriate to leave this decision in the hands of the platform. However, in Global South countries with evolving rule of law thresholds and governments who may seek to leverage platforms to drive their political agenda and spread misinformation, it may not be optimal to empower the government to make such a decision. The most appropriate approach may seem to be setting up an independent panel of experts and academics. However, these stakeholder groups are already overburdened and stretched for resources in Global South countries and consequently may not have the capacity to take on such a responsibility. Careful thought has to be given to designing an optimal policy solution that enables effective researcher access. This in turn can enable greater platform transparency and hence generate informed public discourse around the design of effective regulatory frameworks to address the underlying causes of harm driven by these platforms.

4 CONCLUSION: OPPORTUNITY FOR INDIA TO LEAD THE WAY FOR THE GLOBAL SOUTH

The Global South has seen the proliferation of misinformation that negatively impacts marginalized and vulnerable users and is detrimental to democratic discourse in these societies. Various regulatory approaches—ranging from speech regulation to intermediary liability to platform self-regulation to co-regulation—are emerging across the globe. Many of these are band-aid solutions and do not address the root causes of the spread of misinformation.

The architecture and design, as well as the revenue models, of internet platforms are key factors that contribute to the spread of misinformation. The reliance of internet platforms on advertising revenue incentivizes them to prioritize content that maximizes user engagement with the platform. However, the prioritization of user engagement as a metric enables internet platforms to become conduits for the spread of misinformation. The more users engage with such misinformation, the more the incentive for platforms to enhance its visibility to more users, accelerating its proliferation. Therefore, since platforms develop their content-delivery algorithms based on such incentives, it is key that transparency and accountability mechanisms for these algorithms be built into regulation.

However, it is important to acknowledge that given the complexity of the algorithms platforms deploy, more information on the algorithms themselves may lead to access to a great deal of incomprehensible data that would have to undergo significant processing to provide meaningful insights. Even this may not clarify the decision-making process or provide meaningful insight into how the algorithms of these platforms operate (Perel & Elkin-Koren, 2016). Another challenge in enabling meaningful information and transparency may emerge from a need to effectively balance privacy and intellectual property considerations (Wachter et al., 2018).[6] While transparency is an important goal in starting to tackle challenges such as misinformation, we do need to keep in mind that there will be competing considerations and trade-offs that will have to be accounted for and balanced against as it is operationalized. Transparency around content moderation practices, advertising, and algorithmic functioning are important to support public debate and understanding around the role and power of platforms. This in turn would hopefully enable conversations around how platforms need to evolve or mechanisms such as middleware need to be adopted.

5 RECOMMENDATIONS

The Indian government is currently redesigning India's Information Technology Act. There is no information available in the public domain on the approaches to platform regulation it is considering. Key recommendations for the government to consider as they redesign the legislation include:

1. *Need for transparency*
   It is important for the government to incorporate transparency measures such as platform information disclosures, enhanced algorithmic transparency by platforms, and mechanisms for researcher access to information from platforms. This will enable regulators, researchers, and civil society organizations to better understand the role of internet platforms in the spread of misinformation and to design optimal policy solutions going forward. Additionally, it will empower the public to comprehend the role and impact of platforms and shape the discourse on how platforms and regulations around them need to evolve.

2. *Information disclosure by platforms*
   There is significant information asymmetry between platforms and other stakeholders, and there is limited information available in the public domain on the functioning of platforms, their business models, and their systems of algorithmic decision-making. Even when information is available, the detail and kind of information available in these sources is varied, challenging to compare, or lacking adequate context to derive meaningful insights. It is important that multistakeholder consultations be undertaken in India to identify the categories of information possibly relevant in the Indian context that platforms should

6 Platforms, for instance, raise the possibility of competitors reverse-engineering their automated techniques.

be required to disclose. At the same time, these consultations can start to develop broad consensus on disclosure formats that will facilitate comparative analysis across platforms. The categories and types of information relevant in the Western context may not necessarily be the same in the Indian context, and platform transparency conversations need to be contextualized within the Indian environment and challenges.

3. *Algorithmic transparency*
   In the context of algorithmic transparency, the redesigned IT Act could require platforms to disclose information on how algorithms work and when they are used, how these algorithms are developed, the logic of the model or overall design, and the factors relevant to the functioning of the algorithm such as data points. A significant question to address is to which stakeholders such disclosures of information should be made and to what extent information should be shared with each category of stakeholders. Platforms' concerns around proprietary information and confidential business strategies need to be considered while designing these disclosure mechanisms. A graded system of disclosure can be adopted, with detailed disclosure to regulators and the basic levels of disclosure to the general public. Algorithmic audits and public scoring systems on platform transparency can be deployed to enhance public trust in platforms and enhance stakeholder understanding of these systems.

4. *Researcher access to information*
   Western countries have seen the rollout of mechanisms for researcher access to information on platforms. However, this has not been true in the Global South context. The IT Act should explore mechanisms to incentivize and enable researcher access to information on platforms. Careful thought has to be given to designing mechanisms that enable effective researcher access and deciding whether regulators, government, platforms, academics and experts, or a hybrid of these entities is best placed to operationalize such access effectively.

The Global South and emerging economies are increasingly adopting regulatory frameworks based on legislative approaches that India adopts, thereby placing a special responsibility on India to carefully consider how it will tackle the challenge of misinformation on internet platforms. As India redesigns its Information Technology Act that regulates internet platforms, the country must adopt regulation that requires transparency measures, enabling accountability and meaningful access to information. India has the technological expertise, regulatory capacity, and engagement with platforms to enable this. In addition to transparency and information disclosures, audits and impact assessments will empower key stakeholders such as regulators and researchers to better understand the system of information flows on internet platforms and the design elements of these platforms that enable the virality of misinformation. This will in turn lay the foundation for regulators and governments to design effective regulatory frameworks that ensure greater algorithmic transparency and accountability and that nudge business models away from overreliance on targeted behavioral advertising and user engagement. These regulations will make a start toward tackling the challenge of misinformation.

REFERENCES

Agarwal, A. (2021a, March 15). Traceability and End-to-End Encryption Cannot Co-exist on Digital Messaging Platforms: Experts. *Forbes India.* https://www.forbesindia.com/article/take-one-big-story-of-the-day/traceability-and-endtoend-encryption-cannot-coexist-on-digital-messaging-platforms-experts/66969/1

Agarwal, A. (2021b, March 17). Can Traceability And End-to-End Encryption Co-exist? Here's the Legal View. *Forbes India*. https://www.forbesindia.com/article/take-one-big-story-of-the-day/can-traceability-and-endtoend-encryption-coexist-heres-the-legal-view/67001/1

Alawadhi, N. (2021, November 1). Tracing originator of message won't break encryption, says MeitY. *Business Standard News*. https://www.business-standard.com/article/economy-policy/tracing-originator-of-message-won-t-break-encryption-says-meity-121110200060_1.html

Algorithmic Accountability Act, H.R. 2231, 117th Cong. (2022). https://www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202022%20Bill%20Text.pdf

Algorithmic Justice and Online Platform Transparency Act, MUR21415 5NT, 117th Cong. (2021). https://www.markey.senate.gov/imo/media/doc/ajopta.pdf

Ananny, M. & Crawford, K. (2018). Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability. *New Media & Society, 20*(3), 973–89. https://doi.org/10.1177/1461444816676645

Arun, C. (2019). AI and the Global South: Designing for Other Worlds. In Dubber, M., Pasquale, F., and Das, S. (Eds.), *The Oxford Handbook of Ethics of AI*. Oxford University Press.

Aryan, A. (2021, May 29). Ravi Shankar Prasad: "Govt not in favour of breaking WhatsApp's encryption, users have full right to it." *The Indian Express*. https://indianexpress.com/article/india/ravi-shankar-prasad-whatsapps-encryption-it-rules-privacy-7334870/

Bahri, C. (2018, December 3). *Interview: Why police still make arrests under IT act Section 66A, years after it was struck down.* Scroll.in. Retrieved June 29, 2022, from https://scroll.in/article/904317/interview-why-police-still-make-arrests-under-it-act-section-66a-years-after-it-was-struck-down

Banning Surveillance Advertising Act of 2022, S.3520, 117th Cong. (2022). https://www.congress.gov/bill/117th-congress/senate-bill/3520/text?r=1&s=1

Barnhart, Brent. (2021, March 26). *Everything You Need to Know about Social Media Algorithms.* Social Sprout. Retrieved June 29, 2022, from https://sproutsocial.com/insights/social-media-algorithms/

Benkler, Y., Faris, R., & Roberts, H. (2018) *Network Propaganda*. Oxford University Press.

Çela, E. (2015). Social media as a new form of public sphere. *European Journal of Social Sciences Education and Research, 4*(1), 195–200. https://doi.org/10.26417/ejser.v4i1.p195-200

Crain, M. & Nadler, A. (2019). Political Manipulation and Internet Advertising Infrastructure. *Journal of Information Policy, 9*, 370–410. https://doi.org/10.5325/jinfopoli.9.2019.0370

Diakopoulos, N., & Koliska, M. (2016). Algorithmic Transparency in the News Media. *Digital Journalism, 5*(7), 809–828. https://doi.org/10.1080/21670811.2016.1208053

European Commission. (2018). *Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation

European Commission. (2020, September). *Assessment of the code of practice on disinformation – achievements and areas for further improvement*. European Sources Online. Retrieved June 28, 2022, from https://www.europeansources.info/record/assessment-of-the-code-of-practice-on-disinformation-achievements-and-areas-for-further-improvement/

European Parliament, Council of the European Union. (2020a). *Commission Proposal 2020/0361 (COD), Regulation on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC*. https://www.europarl.europa.eu/cmsdata/244857/2020%200361(COD)-09h19-28_01_2022.pdf

European Parliament, Council of the European Union. (2020b). *Commission Proposal 2020/0374 (COD), Regulation on contestable and fair markets in the digital sector (Digital Markets Act).* https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN

General Data Protection Regulation 2016/679, 13–15. (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

George, Cherian. (2018, December 18). *Divisive Disinformation and the Hate Spin Dilemma. Centre for Media Risk*. Center for Media at Risk. Retrieved June 29, 2022 from www.ascmediarisk.org/2018/12/cherian-george-divisive-disinformation-and-the-hate-spin-dilemma/

Habermas, J. (1962). *The structural transformation of the public sphere: An inquiry into a category of bourgeois society.* MIT Press.

Horwitz, J. (2021a, October 1). The Facebook Files. *Wall Street Journal.* Retrieved June 29, 2022, from www.wsj.com/articles/the-facebook-files-11631713039

Horwitz, J. (2021b, October 3) The Facebook Whistleblower, Frances Haugen, Says She Wants to Fix the Company, Not Harm It. *Wall Street Journal.* Retrieved June 29, 2022, from www.wsj.com/articles/facebook-whistleblower-frances-haugen-says-she-wants-to-fix-the-company-not-harm-it-11633304122?mod=article_inline

Human Rights Watch (2018, February 14). *Germany: Flawed social media law.* Retrieved June 28, 2022, from https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law

Human Rights Watch (2019, April 3). *Singapore: Reject sweeping "fake news" bill.* Retrieved June 28, 2022, from https://www.hrw.org/news/2019/04/03/singapore-reject-sweeping-fake-news-bill

Indian Penal Code, 1860. (1860). https://legislative.gov.in/sites/default/files/A1860-45.pdf

Information Technology Act, 2000. (2000). https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. (2021). https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf

Ireton, C., Posetti, J., & Fadil, A. (2018). *Journalism, 'fake news' & disinformation.* UNESCO. Retrieved June 28, 2022 from https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf

Isaac, M. (2021, October 25). Facebook Wrestles With the Features It Used to Define Social Networking. *The New York Times*. https://www.nytimes.com/2021/10/25/technology/facebook-like-share-buttons.html

Jones, K., Libert, K., & Tynski, K. (2016, May 23). The Emotional Combinations That Make Stories Go Viral. *Harvard Business Review*. https://hbr.org/2016/05/research-the-link-between-feeling-in-control-and-viral-content

Keller, D., & Leerssen, P. (2019). Facts and Where to Find Them: Empirical Research on Internet Platforms and Content Moderation. In N. Persily & J. Tucker (Eds.), *Social Media and Democracy: The State of the Field, Prospects for Reform*. Cambridge: Cambridge University Press.

Retrieved from https://papers.ssrn.com/abstract=3504930

Little, O. (2021, March 3). *TikTok is prompting users to follow far-right extremist accounts.* Media Matters for America. https://www.mediamatters.org/tiktok/tiktok-prompting-users-follow-far-right-extremist-accounts

Llansó, E., van Hoboken, J., Leersen, P., & Harambam, J. (2020). *Artificial intelligence, content moderation, and freedom of expression.* Transatlantic Working Group on Content Moderation Online and Freedom of Expression. Retrieved March 2, 2020, from https://www.ivir.nl/publicaties/download/AI-Llanso-Van-Hoboken-Feb-2020.pdf

Mathi, S. (2022, April 27) *Draft Of IT Act Replacement Law Will Be Out In May: IT Minister Rajeev Chandrasekhar.* Medianama. https://www.medianama.com/2022/04/223-it-act-replacement-draft-timeline/

Mayor, K. (2019, August 16). Fair competition and transparency benefits us all. Newsroom | TikTok. https://newsroom.tiktok.com/en-us/fair-competition-and-transparency-benefits-us-all

Ministry of Electronics and Information Technology, Government of India (MeitY). (2021). Frequently Asked Questions (FAQs) on Part II of the Information Technology (Intermediary and Digital Media Ethics Code) Rules, 2021. https://www.meity.gov.in/writereaddata/files/FAQ_Intermediary_Rules_2021.pdf

Ministry of Electronics and Information Technology, Government of India (MeitY). (2022). Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022. https://egazette.nic.in/WriteReadData/2022/239919.pdf

Ministry of Electronics and Information Technology, Government of India (MeitY). (2023). Proposed amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2021. https://www.meity.gov.in/writereaddata/files/Revised-IT-Rules-2021-proposed-amended.pdf

Nadler, A., Crain, M., & Donovan, J. (2018). *Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech.* Data & Society. https://datasociety.net/wp-content/uploads/2018/10/DS_Digital_Influence_Machine.pdf

Network Enforcement Law, Bundestag (Germany). (2017). https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2

Neyazi, T. A. (2019). Digital propaganda, political bots and polarized politics in India. *Asian Journal of Communication, 30*(1), 39–57. https://doi.org/10.1080/01292986.2019.1699938

Perel (Filmar), M., & Elkin-Koren, N. (2016). Black Box Tinkering: Beyond Transparency in Algorithmic Enforcement. *Florida Law Review, 69,* 181-221. https://doi.org/10.2139/ssrn.2741513

Press Trust of India (PTI). (2019, November 21). Govt finalising IT rules for Social Media to trace original source of Info. *Business Standard.* Retrieved June 29, 2022, from https://www.business-standard.com/article/pti-stories/govt-finalising-new-it-rules-for-social-media-entailing-traceability-of-info-originator-119112101042_1.html

Press Trust of India (PTI). (2021, October 23). Centre Defends IT Rule Requiring WhatsApp to Trace Originator of Message. NDTV. https://www.ndtv.com/india-news/centre-defends-it-rule-requiring-whatsapp-to-trace-originator-of-message-2584850

Privacy International. (2017, August 30). Case Study: Profiling and Elections - How Political Campaigns Know Our Deepest Secrets. https://privacyinternational.org/case-study/763/case-study-profiling-and-elections-how-political-campaigns-know-our-deepest-secrets

Protection from Online Falsehoods and Manipulation Act 2019 (2019). https://sso.agc.gov.sg/Acts-Supp/18-2019

Rajan, N. (2021, May 26). WhatsApp moves Delhi HC against traceability clause in IT rules, calls it is unconstitutional. *The Indian Express.* https://indianexpress.com/article/technology/tech-news-technology/whatsapp-moves-delhi-high-court-over-traceability-clause-social-media-rules-7330558/

Ranking Digital Rights. (2020). It's the Business Model: How Big Tech's Profit Machine is Distorting the Public Sphere and Threatening Democracy. https://rankingdigitalrights.org/its-the-business-model/

Reuters. (2018, December 7). *WhatsApp asked by government to trace origin of messages spreading misinformation- technology news.* Firstpost. Retrieved June 29, 2022, from https://www.firstpost.com/tech/news-analysis/whatsapp-asked-by-government-to-trace-origin-of-messages-spreading-misinformation-5693031.html

Shreya Singhal v. Union of India (2015) 5 SCC 1, ¶ 122.

Social Media NUDGE Act, S. 3608, 117th Cong. (2022). https://www.congress.gov/117/bills/s3608/BILLS-117s3608is.pdf

Turcilo, L. & Obrenovic, M. (2020, August). *Misinformation, disinformation, malinformation: Causes, trends, and their influence on democracy.* Heinrich Böll Foundation. Retrieved June 28, 2022, from https://hk.boell.org/sites/default/files/imported-Files/2020/11/04/200825_E-Paper3_ENG.pdf

Vaidhyanathan, S. (2018). *Antisocial media: How Facebook disconnects Us and Undermines Democracy.* Oxford University Press.

Vincent, J. (2022, April 23). Google, Meta, and others will have to explain their algorithms under new EU legislation. *The Verge*. https://www.theverge.com/2022/4/23/23036976/eu-digital-services-act-finalized-algorithms-targeted-advertising

Wachter, S., Mittelstadt, B., Russell, C., Allo, P., Burk, D., Bygrave, L., Hildebrandt, M., Landsberg, D., Lipton, Z., Spina, A., Sutcliffe, D., Thompson, J., Wand, J., & Zarsky, T. (2018). Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology, 31*, 841. Retrieved from https://doi.org/10.48550/arXiv.1711.00399

Woolley, S. & Howard, P. (2018). *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford University Press.

Wu, L., Morstatter, F., Carley, K., & Liu, H. (2019, December). Misinformation: Definition, Manipulation, and Detection. *ACM SIGKDD Explorations Newsletter, 21*(2), 80-90.

The New Face of Techno-Authoritarianism: How Emerging Economies are Shaping the Rules of International Digital Governance to Their Advantage

Danielle Youlan Luo and Panthea Pourmalek

ABSTRACT:

This paper homes in on two unique trends in the current course of digital governance—techno-nationalism and techno-authoritarianism. The first trend points to emerging norms of data localization and centralization among emerging economies, rooted in techno-nationalist domestic and foreign policies. The second trend captures the use of technology-enabled authoritarian tactics—ranging from data grabs, surveillance, misinformation, and targeted political campaigns, to internet shutdowns—to significantly enhance the power of the state and undermine political freedoms. This paper argues that techno-nationalist, state-led digital centralization, data localization, and infant tech industry protection may have paved the way for a new form of techno-authoritarianism in democratic emerging economies led by authoritarian-leaning governments. As a result, techno-authoritarian practices are embedded in laws and institutions and are thus more powerful, dangerous, and enduring. Based on case study analyses of India and Brazil, this paper concludes with policy recommendations oriented at strengthening domestic data protection in authoritarian-leaning democracies, and capitalizing on shared principles and existing connections to steer peer democracies toward cooperation on global digital governance efforts.

KEYWORDS: Techno-nationalism, techno-authoritarianism, emerging economies, data localization, privacy, global digital governance

1 INTRODUCTION

The newest era of rapid digitalization presents a new front of strategic competition—between countries wanting to reap the benefits of data-driven technological innovation and a rapidly expanding digital economy. This paper homes in on two unique trends in the current course of digital governance—techno-nationalism and techno-authoritarianism. The first trend points to norms of data localization among emerging economies, rooted in techno-nationalism. Countries like India, Brazil, Indonesia, and South Africa face a double bind—tasked with protecting large populations from new and real risks of datafication while also facing intense competition with other states in capturing the untapped potential of a new wave of technologies. Rather than leaving the rulebook of digital governance to established players like the United States (U.S.) and the European Union (EU), or major challengers like China, emerging economies have grown increasingly assertive in securing their strategic interests in the

formation of these new global norms. Attempts to keep up with the first-mover advantage of mature digital economies, which have established norms of governance that protect their market share and access to data, have manifested as domestic legislation that is pro-data localization and supports indigenous tech ecosystems in ways akin to known strategies of infant industry protection. Paired with the rhetoric of national security, the approach of key emerging economies to data governance has taken on a strong techno-nationalist character.

The second trend points to an erosion of privacy and democratic rights in major democratic emerging countries like India and Brazil, where the lines between techno-nationalism and techno-authoritarianism are increasingly blurred. Policies for data localization and protection of budding tech industries coincide with techno-authoritarian moves. From data grabs, surveillance, misinformation, and targeted political campaigns, to internet shutdowns, techno-authoritarianism takes on a wide range of forms—all boiling down to using technology to achieve a highly asymmetrical power distribution between the state and its people. While discussed in detail in the literature on the Chinese digital economy, the increasing presence of techno-authoritarianism in otherwise democratic systems has not attracted the same attention.

This paper interrogates the increasing preference for data localization and market protection, questioning if protectionist, state-led digital centralization has inadvertently created fertile conditions for the authoritarian seed to germinate in democratic emerging economies. To enact protectionist digital policies, governments occupy the driver's seat of digital legislative infrastructure and industrial relations—enduring elements that can drastically enhance a state's capacity for digital control. In contrast to other literature on techno-authoritarianism, this paper focuses on democracies with authoritarian-leaning leadership and administration. It argues that competition-bred techno-nationalism, including data localization and infant tech industry protection, may have paved the way for a new form of techno-authoritarianism in democratic emerging economies led by authoritarian-leaning governments. Using India and Brazil as case studies, it demonstrates that the impact of enhanced digital control capacity goes beyond providing a more level playing field for emerging economies in the digital realm: it also lays the ground for imprudent use of data and technologies to curb dissent, shape political narratives—and even determine democratic outcomes.

2 LITERATURE REVIEW: Understanding Techno-Nationalism and Techno-Authoritarianism

To understand this new nexus between techno-nationalism and techno-authoritarianism, it is necessary to establish the conceptual parameters for each phenomenon. The key traits of techno-nationalism and techno-authoritarianism are outlined in Table 1 in the Appendix.

2.1 TECHNO-AUTHORITARIANISM

Some authors define techno-authoritarianism as the use of technology as a tool for enhancing existing authoritarian systems (Sherman, 2021) or by authoritarian leaders (Yayboke & Brannen, 2020). Others emphasize an inherent administrative and institutional effort (Lilkov, 2020, p. 61) and "the use of technology by authoritarian governments not only to control, but to shape the behavior of its citizens" (Khalil, 2020, p. 6). Across all definitions, the ultimate objective of techno-authoritarianism is to maintain and solidify political control—by authoritarian systems, regimes, or leaders.

There exist three key mechanisms for techno-authoritarianism. The first is *limiting access to digital information.* This can be done by cutting off access to digital platforms through electricity, internet, or cellular service shutdowns; by restricting access to foreign content (Sherman 2021); or by complete internet isolation (Howells & Henry, 2021). Second is *censorship and the manipulation of public opinion.* While direct censorship is a key mechanism for techno-authoritarianism (Yayboke & Brannen, 2020; Cebul & Pinckney, 2021; Howells & Henry, 2021; Jamil, 2021; Pearce & Kendzior, 2012; Khalil, 2020; Lilkov, 2020; Sherman, 2021), indirect censorship through the manipulation of public discourse and opinion is an equally important—and

perhaps more banal—exercise of techno-authoritarianism. Control of discourse is conducted in online and digital spaces in the name of preventing the spread of fake news (Lilkov, 2020; Sherman, 2021), through state-led misinformation and disinformation (Yayboke & Brannen, 2020; Cebul & Pickney, 2021; Khalil, 2020), and government-led creation of fake posts on social media (Lilkov, 2020). The final mechanism is the *monitoring and surveillance of online activity*, done by monitoring online traffic and IP addresses (Sherman, 2021) and social media activity (Lilkov, 2020). Other manifestations of techno-authoritarianism can be seen in the control of digital financial systems (Fanusie & Jin, 2015) and electoral manipulation (Yayboke & Brannen, 2020).

The literature on techno-authoritarianism is focused primarily on China (Fanusie & Jin, 2021; Khalil, 2020; Lilkov, 2020) and other contexts with existing authoritarian or authoritarian-leaning regimes, including Russia (Howells & Henry, 2021), post-Soviet states like Kazakhstan (Anceschi, 2015) and Azerbaijan (Pearce & Kendzior, 2012), the Arab world (Galal & Shehata, 2020), Pakistan (Jamil, 2021), and Zimbabwe (Mare, 2020).

A handful of scholars point to the significance of digital data in techno-authoritarianism. Here, the institutionalization of the data transfer from private to public entities (Khalil, 2020; Lilkov, 2020), facilitated through data localization policies (Yayboke & Brannen, 2020), is a key trait of modern techno-authoritarianism that will be explored in greater detail by the case studies presented in this paper.

2.2 TECHNO-NATIONALISM

The conceptual boundaries of techno-nationalism can be more nebulous. In the absence of strict definitions, four common mechanisms have been identified across literature on techno-nationalism. The first is *creating national identity and realities through the nationalization and territorialization of digital and information infrastructure.* The datafication of populations, even in conventional ways like census data collection, transforms people into "national" populations (Möllers, 2021). The construct of internet domains and digital ecosystems supplements this process by creating a digital counterpart to the nation-based territory (Mihelj & Jiminez-Martinez, 2021; Möllers, 2021). More recently, biased algorithms and search engines (e.g., Baidu vs. Google) work to shape realities based on personal, political, and economic attributes (Gillespie, 2014; Mihelj & Jiminez-Martinez, 2021; Schneider, 2018). Second is *state-led technology development and innovation.* Here, the state takes the lead in national innovation systems (Kim et al., 2020) and assumes a significant role in the technological standardization process—as a "project founder, risk undertaker, interest moderator, collaboration facilitator, and process monitor" (Gao et al., 2014).

In techno-nationalist systems, national technology and innovation policy is formed to avoid or minimize dependence on foreign technologies.

The third mechanism is the *nurturing and growth of domestic technology champions.* In techno-nationalist systems, the government requires domestic firms to follow specific and unique standards for commercial success, thus steering companies and commercial activities in a direction that stimulates national economic growth and wealth creation (Kim et al., 2020). National technology and innovation policy is formed to avoid or minimize dependence on foreign technologies (Kohno, 1995) and protect local firms from international competition by banning their international counterparts (Lilkov, 2020). The fourth and final mechanism is outward-oriented and necessitates the *international expansion of domestic firms and domestic-made digital infrastructure and standards.* This dimension is especially visible in the Chinese case, with interests in standardization of information and communication technologies (ICTs), integration into global markets, global acceptance of indigenous tech standards, and overseas expansion of Chinese digital infrastructure (e.g., Huawei) (He, 2022; Kim et al., 2020).

Techno-nationalism can be broken down into two subcomponents: *political-informational* and *political-economic.* Political-informational techno-nationalism is closely connected to nationalist populism, relies on the control of information to gain and maintain popular political support, and occurs mainly at the domestic level. In many cases, this face of techno-nationalism is intimately connected to techno-authoritarianism, as discussed in the Brazil case study. On the other hand, political-economic techno-nationalism makes use of politics to support nationalist tech policies, and vice versa. This phenomenon occurs at both domestic and state levels. The domestic-international interface is necessary for political-economic techno-nationalism. For example, India used nationalist rhetoric connected to the death of Indian soldiers in 2020 border clashes with China as justification for banning numerous Chinese applications (Kynge, 2020; "India Bans Dozens of Chinese Apps," 2020). Since then, TikTok's home-grown counterpart JOSH has gained popularity in India (Rai, 2022), highlighting the use of geopolitical tensions to ban foreign tech platforms in favor of growing domestic ones.

3 THE MERGING OF TECHNO-NATIONALISM AND TECHNO-AUTHORITARIANISM IN DEMOCRACIES

Despite the focus of the above body of literature on existing authoritarian systems, techno-nationalism and techno-authoritarianism in *democracies with authoritarian-leaning leadership* may be an emerging trend and cause for concern. The heightened strategic importance of technology, particularly those reliant on digital data, has ushered in a new wave of techno-nationalist policies. In pursuing them, democracies create fertile ground for techno-authoritarian moves with the potential to be embedded in laws and institutions. The India and Brazil case studies trace the emergence of techno-nationalism and techno-authoritarianism under authoritarian-leaning leaders Narendra Modi and Jair Bolsonaro—known for their erosion and undermining of democratic systems. While similar trends are also present in liberal democracies such as the United States, the extent to which techno-authoritarianism is instituted through legislative means is not the same as they are in authoritarian-leaning democracies.

3.1 CASE STUDY: INDIA

There is no better illustration of India's turn to techno-authoritarianism than the crackdown on online public discourse and government-led digital surveillance during the 2020–2021 farmers' protests. In February 2021, areas near protest sites faced several rounds of government-mandated internet shutdowns (Mitra & Hollingsworth, 2021). In the same month, Twitter received orders from the Indian government to remove hundreds of accounts with activity related to the protests, with which the social media giant initially complied (Iyengar, 2021). In another case, Indian police requested information from Google and other platforms on users who engaged with a toolkit on digital organizing shared by climate activist Greta Thunberg (Ghosh, 2021). In response, ten globally known nonprofit organizations issued a public call to the Indian government to cease protest-related digital surveillance and censorship ("Indian Government Must Correct Moves," 2021).

While initially complacent, social media platforms eventually pushed back against the strong-arming by the Indian government. In June 2021, WhatsApp sued the Indian government over provisions in the *Intermediary Guidelines and Digital Ethics Code* that required platforms to share the first originator of messages, effectively breaking WhatsApp's end-to-end encryption (Freedom House, 2022; Isaac, 2021). Following temporary compliance with Indian governmental orders, Twitter restored access to most affected accounts and released a public statement emphasizing the right of free expression on the platform (Twitter Safety, 2021). These requests were made according to another controversial

law—section 69A of the Information Technology Act, which allows blocking access to telecom, online, and digital services in the name of sovereignty, security and defense, and friendly relations with foreign states (Law No. 21, 2000). It is worth noting that despite this resistance, Twitter opted to withhold access to a number of initially blocked accounts within India, even as they were available to access from outside the country.

The events of the farmers' protests are not isolated and appear to be symptomatic of a more significant trend. Access Now recorded 106 instances of internet shutdowns in India in 2021 alone, a whopping 91 cases ahead of Myanmar, with the second greatest number of shutdowns at 15 (Diaz Hernandez & Anthonio, 2022). Internet shutdowns and limiting access to online connectivity were used previously in 2019 and 2020 in Jammu and Kashmir (Freedom House, 2021). Surveillance of digital content and discourse also appears to be on an upward trend. Prior to the peak of protests, India had submitted 10,000 tweet removal requests to Twitter in 2020, a major increase from 1,200 requests in 2019, and only 248 in 2017 (Soni, 2021). The use of Pegasus spyware for government surveillance of opposition figures, activists, and journalists was leaked as part of the 2021 "Pegasus Project" investigations (Freedom House, 2022; Varadarajan, 2021).

India, particularly under Modi's rule, exhibits many classic symptoms of techno-authoritarianism. It also serves as an excellent case study to illustrate the rise of techno-nationalist policies leveraging the massive value of digital data. During the 2019 G20 summit, former Japanese Prime Minister Abe introduced the idea of the "Osaka Track" and its core principle of "Data Free Flow with Trust" (DFFT)—produced through earlier plurilateral negotiations between developed countries, including the U.S., EU, Australia, Japan, and Singapore (Sugiyama, 2019; Hufbauer & Lu, 2019, p. 1). India opted to reject the Osaka Track alongside Indonesia and South Africa (Taliyan, 2019)—a major turning point for a previously passive participant in international digital governance.

India's approach to international digital and tech governance is largely shaped by an inability to capitalize fully on previous rounds of industrialization. While India has shown aptitude in the realm of information technology (IT), it has largely served as a destination for tech outsourcing (Determann & Gupta, 2019, p. 131). By virtue of a large population, Indians produce large quantities of digital data that serve as a source of profit for foreign tech firms. At the same time, India has shown increasingly promising technological prowess. When surveyed, global tech industry leaders, experts, and investors ranked India third in showing "most promise for developing globally impactful disruptive technologies," following behind the U.S. and China with increasingly small margins (KPMG, 2018, 2020).

In response to a perception that countries with established technological prowess will demand access to the data of populous nations, India has oriented itself as a proponent of data localization norms. The Indian demand for unrestrained development in the data realm is reminiscent of broader ideologies employed by industrializing or developing countries and parallels strategies like infant industry protection. Like other developing countries, India hopes to use data localization as a means of "[exercising] economic ownership" of Indian data (Yakovleva & Irion, 2020, p. 203) and empowering its own companies to become globally competitive before exposing them to free data flows (Taliyan, 2019).

Techno-nationalist rhetoric and approaches are also increasingly embedded in the Indian bureaucracy. An internet search for "Osaka Track" returns numerous instructional videos for individuals preparing for India's yearly Civil Service Examination that detail the advantages and disadvantages of the Osaka Track for emerging and industrializing economies. Such sources stress that India will protect its "policy space" for digital industrialization by resisting similar plurilateral attempts in the future, opting instead to push discussions under the WTO Work Programme on E-Commerce (ALS TargetMains, 2019; Civil Service School, 2021). Using language like "digital colonialism," they hint at a significant ideological underpinning to the Indian approach—one that connects international tech and data governance to radical visions of Indian nationalism.

India's engagement with the Osaka Track proposal, and, more broadly, the governance of cross-border data flows, exemplifies *political-economic techno-nationalism*.

At the domestic level, India introduced the *Personal Data Protection Bill* (PDPB) in 2019, following a key supreme court judgment on the right to privacy in India. While similar to the *EU General Data Protection Regulation* (GDPR) in its inception, the PDPB was remarkable for its inclusion of data localization provisions. After four years of parliamentary review and multiple revisions to the bill, the PDPB was withdrawn as of August 3, 2022. A new data protection bill that better fits into existing legal framework will be tabled in the first quarter of 2023. The latest version of the bill before its August withdrawal retained provisions for localization of loosely defined "critical personal data." More concerningly, Clause 35 of the 2021 bill exempts government agencies from nearly all parts of the law (*The Data Protection Bill,* 2021). Should the new 2023 bill retain or mimic Clause 35, the government would be legally allowed to not comply with the new privacy protection bill. In addition, the Modi government's draft *India Data Accessibility and Use Policy,* first released in February 2022, was criticized for its proposed licensing and potential sale of government-held data to the private sector. A substitute draft, *National Data Governance Framework Policy,* as shared in May 2022, instead proposes an ambitious platform to centralize government-collected nonpersonal or anonymized data and streamline its use by private actors. Despite a comparatively moderate approach, technical details regarding data anonymization remain unclear, and the policy's potential implementation in the absence of a strong data protection bill remains an area of concern. With the Modi government's increasingly authoritarian turn and disregard for legal and democratic norms, government exemption from the country's data and privacy law is a major concern.

Aadhar, a biometric identification megaproject introduced in 2009, illustrates the Indian government's imprudent and careless approach to large-scale data collection. With over a billion users, *Aadhar* may be the world's largest centralized governmental data collection project. During its initial rollout, the program was not grounded in any legal privacy or data protection frameworks—garnering major criticism and concern (Dixon, 2017; Prasad & Menon, 2020, p. 12). Despite legal improvements in privacy since 2009, the massive biometric database is a cause for concern when in the hands of an increasingly authoritarian regime. In 2022, a High Court justice publicly suggested the use of a legal loophole to use *Aadhar* biometric data for a police murder investigation (Hersey, 2022). Major government-led data collection projects are increasingly common for governments aiming to harness the value of high-quality personal and digital data. The Indian government's practical disregard for data privacy creates a clear risk of such techno-nationalist megaprojects being used for techno-authoritarian ends.

The Indian government's practical disregard for data privacy creates a clear risk of techno-nationalist megaprojects being used for techno-authoritarian ends.

3.2 CASE STUDY: BRAZIL

The case of India verifies this paper's initial hypothesis by demonstrating that protectionism-driven techno-nationalism enables techno-authoritarian practices. A closer look at the case of Brazil shows that even in the absence of a rapidly expanding digital economy and digital

protectionism, the political-informational variant of techno-nationalism can also encourage data grabs and unleash techno-authoritarian forces.

Prior to the election of President Jair Bolsonaro, Brazil had significant experience with government-led data collection and data sharing, as well as some data protection policies (Filgueiras & Lui, 2022). In 2014, Brazil demonstrated notable leadership by backing the NETmundial Initiative—an international initiative to develop an internet governance framework. Despite sustaining a highly progressive track record in digital governance, Brazil's approach to digital policies took a sharp turn with the election of Bolsonaro. In 2019, a decree issued by Bolsonaro mandated the creation of a data registry known as the *Cadastro Base do Cidadão* (CBC) in the name of enhancing the efficiency of Brazil's public sector (Kemeny, 2020; Mari, 2019), which marked a turning point in Brazil's government-led use of big data. The CBC is a single master database that centralizes 50 existing datasets held by federal agencies and departments, with information on over 200 million Brazilians (Lefèvre & Souza, 2020; Mari, 2019). The data included ranges from typical personal information such as name, date of birth, and gender, to higher-order and more sensitive data like social security and voting card numbers, health data (medical history, genetic sequencing) and an expanded category of biometric data such as palm print, fingerprint, retina or iris, facial configuration, voice, and gait (Decree No. 10.046, 2019; Mari, 2019). Under the decree, all federal bodies face no barriers to acquiring the full range of data, as they now share access to a common and expanded database. It is important to recognize that the CBC was created at a time when the Brazilian government was already engaged in mass collection of health data due to the pandemic—the Ministry of Health was granted expanded authority to collect and maintain a wide range of health data, and multiple levels of governments began collecting geolocation data to verify isolation status (Lefèvre & Souza, 2020). The absence of public consultation and the high degree of opacity throughout the CBC's conceptualization and implementation (Kemeny, 2020) raises questions about the intended purpose of pushing through such a controversial measure quickly and quietly.

In addition to supplementing Brazil's pandemic response, the primary objective of the CBC, according to the government, is to modernize and enhance the efficiency of Brazil's public service by facilitating data sharing between different government bodies (Presidência da República, 2019). While the idea of a digital government is attractive, a rich bank of data would also strengthen the state's digital control and enhance its ability to trace, identify, and organize citizens. In essence, the CBC nationalizes population data and mandates state ownership of such data, demonstrating a quintessential case of *political-informational techno-nationalism*. The *Cadastro* presents an example of how centralized data collected without checks and balances in the name of nationalism enables authoritarian-leaning leaders with a powerful repressive tool.

The *Cadastro* presents an example of how centralized data collected without checks and balances in the name of nationalism enables authoritarian-leaning leaders with a powerful repressive tool.

Brazil has demonstrated that this type of techno-nationalism can easily veer into the dangerous ground of techno-authoritarianism. Without citizens' approval or knowledge, Brazil's National Intelligence Agency used the decree to obtain all 76 million copies of driver's license records (Dias & Moro Martins, 2020). The Director of the Agency, Alexandre Ramagem, is a family friend of Bolsonaro's and a known political appointee. A previous attempt to appoint Ramagem as the country's Chief of Police failed amid allegations of Bolsonaro demanding direct access to policy investigations and intelligence ("Bolsonaro taps family friend," 2020). While there is no near-term clarity on how the intelligence agency's data grab would restrict freedom, privacy was undoubtedly compromised. In the long term, a rich and nationalized data bank hosting sensitive personal information can be used to serve techno-authoritarian means by curating targeted political narratives, manipulating election outcomes, and even augmenting realities for different demographics. This is especially concerning in the current Brazilian context, where leaders of powerful agencies with access to centralized citizen data are appointed by and closely affiliated with the country's authoritarian leader.

Despite the *Lei Geral de Proteção de Dados* (LGPD), a data regulatory framework similar to the EU GDPR coming into effect in February 2020, Section 3 Article 4 Chapter 1 of the LGPD stipulates that the legal framework does not apply to the process of personal data collection performed exclusively for public safety, national defense, state security, and investigation and prosecution of criminal offences (Presidência da República, 2018). Such exceptions would inadvertently strengthen public and governmental bodies' control of personal data. In the absence of a robust legal privacy framework that obligates governmental bodies to comply, data collected in the name of techno-nationalism can be transformed easily into a tool for techno-authoritarianism.

Unlike India, a relatively small Brazilian digital economy and the absence of national technology champions render Brazil's practice of techno-nationalism primarily centered around the political-informational aspect, resulting in significantly less techno-nationalist sentiments in Brasilia, driving hard-line legislative efforts that further centralize digital oversight and control as compared to India. India's digital authoritarian practice serves as a precautionary tale as Brazil's level of digitization grows, especially when President Bolsonaro has demonstrated a strong appetite for banal techno-authoritarian strategies such as indirect censorship through the manipulation of public opinion, misinformation, and disinformation during the COVID-19 pandemic (Ricard & Medeiros, 2020).

Evidence from Brazil offers an expanded view of this paper's hypothesis. While political-economic driven techno-nationalism and its associated data protectionism strategies are the primary drivers that enable techno-authoritarianism, the creation and use of the Brazilian *Cadastro* demonstrates that political-informational techno-nationalism is also a palpable contributing force.

Despite the blurred lines between techno-nationalism and techno-authoritarianism in both India and Brazil, both countries' centralized approaches to data collection have not yet enabled clear cases of political manipulation intended to undermine the integrity of democratic processes, nor contributed to large-scale targeted actions against particular demographics. But the absence of both cannot be taken for granted, especially when institutionalized frameworks such as *Aadhar* and the *Cadastro* have already laid fertile ground for data exploitation. While it is intuitive to believe that checks and balances—such as personal data protection laws—could serve as mitigants to the risk of data exploitation, India's DPB and Brazil's LGPD both illustrate the ease of making exceptions for government entities. The objective of digital data regulation, particularly for international tech firms, is used as justification to create self-serving tech policies that advantages and justifies the government in its own authoritarian behavior. Data protection rules now need to keep in check the very government that creates them, creating a Catch-22 that leaves domestic populations vulnerable.

4 CONCLUSION

Techno-authoritarianism is on the rise in some of the world's most populous democracies. This paper contributes to the discourse on this trend by highlighting the role of techno-nationalist policies as an accelerant for techno-authoritarianism. Techno-nationalist policies and programs that focus on guaranteeing government access to digital data or on the protection of domestic tech firms from international competition may create tools of techno-

authoritarianism—inadvertently or intentionally. In this sense, techno-nationalism can create, expand, and enable techno-authoritarian practices that are more powerful, dangerous, and embedded in laws and institutions, as techno-nationalist justifications associated with banal administrative bureaucracy, national security, and economic growth tend to be met with less resistance.

Based on the analysis of the India and Brazil case studies, this paper highlights two areas of concern. First: weak domestic legal landscapes for personal data and privacy protection. Laws that establish rights for data subjects but include exemptions for public bodies are especially concerning in the context of increasing government-led personal data collection initiatives. Second: protectionist approaches that seek to shelter domestic tech firms from international competition and guarantee their access to domestic digital data. Such protectionism is rooted in techno-nationalism and renders countries like India resistant to participation in global governance efforts on cross-border data flows, and technological governance more broadly.

Techno-nationalist sentiments are unlikely to dissipate in the near term, given the backdrop of a fragmented international system and the shared desire among countries to reap the benefits of the digital economy. However, three critical guardrails can be put in place to prevent techno-nationalism from enabling the growth of techno-authoritarianism. First, democracies should support the strengthening of domestic privacy laws with a minimum degree of applicability to government entities, by establishing and recommending basic international ethics of data collection, protection, and use. Ethics have no binding power, but can over time influence acceptable norms and serve as a counterweight to protectionist and nationalist data practices that quietly enhance governments' leverage over citizens. Second, in the absence of space for high-level global governance on the tech front, democracies should aim to develop "rules for co-existence" for the digital economy (Tiberghien et al., 2022). Recognizing the presence of prominent resistant actors like China and Russia, democracies must capitalize on shared principles and existing connections to steer peer democracies toward cooperation, particularly through the creation of Digital Trade Agreements with commitments to digital trade and cooperation in other digital spheres. The more the need and desire for extreme techno-nationalist policies are mitigated, the greater the likelihood of preventing the associated acceleration of techno-authoritarianism. Third, as democracies develop and update their respective data privacy laws, they should aim to achieve an acceptable degree of legal interoperability among various domestic legislations, thereby allowing democracies to share and broaden best practices that minimize techno-authoritarian practices at least, and at best contributing toward converging data laws that pave the way for an organically formed international data governance framework.

For democracies, techno-nationalism and protectionist tech policies should not be a matter of concern only when posing barriers to trade. Democracies should be conscious of the real possibility for techno-nationalism to usher in a long-term erosion of democracy and create institutionally embedded techno-authoritarian tools and practices resistant to change.

Arguments presented in this essay solely represent the view of the authors and do not indicate the view of other institutions associated with the authors.

REFERENCES

ALS TargetMains 2019. (2019, August 9). *Osaka track* [video]. YouTube. https://www.youtube.com/watch?v=K2qx_TgZ_Hk&t=181s

Anceschi, L. (2015). The persistence of media control under consolidated authoritarianism: Containing Kazakhstan's digital media. *Demokratizatsiya*, 23(3), 277–295.

Bolsonaro taps family friend as Brazil's federal police chief. (2020, April 29). *Al Jazeera*. https://www.aljazeera.com/news/2020/4/29/bolsonaro-taps-family-friend-as-brazils-federal-police-chief

Cebul, M., & Pinckney, J. (2021). *Digital authoritarianism and nonviolent action: Challenging the digital counterrevolution*. United States Institute of Peace. https://www.usip.org/publications/2021/07/digital-authoritarianism-and-nonviolent-action-challenging-digital

Civil Service School. (2021, March 6). *Osaka track declaration* [video]. YouTube. https://www.youtube.com/watch?v=KpVyXSeb7-M&t=536s

Determann, L., & Gupta, C. (2019). India's personal data protection act, 2018: Comparison with the general data protection regulation and the California consumer privacy act of 2019. *Berkeley Journal of International Law, 37*(3), 481.

Dias, T. & Moro Martins, R. (2020). Documentos Vazados Mostram Que Abin Pediu Ao Serpro Dadaos E Fotos De Todas As CNHs Do País. *The Intercept*. https://theintercept.com/2020/06/06/abin-carteira-motorista-serpro-vigilancia/

Diaz Hernandez, M., & Anthonio, F. (2022). *The return of digital authoritarianism: Internet shutdowns in 2021*. Access Now. https://www.accessnow.org/cms/assets/uploads/2022/04/2021-KeepItOn-Report-1.pdf

Dixon, P. (2017). A Failure to "Do No Harm"—India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S. *Health and Technology, 7*(4), 539–567. https://doi.org/10.1007/s12553-017-0202-6

Fanusie, Y. J., & Jin, E. (2021). *China's digital currency: Adding financial data to digital authoritarianism.* Center for a New American Security. https://www.cnas.org/publications/reports/chinas-digital-currency

Filgueiras, F., & Lui, L. (2022). Designing data governance in Brazil: An institutional analysis. *Policy Design and Practice*, 1–16. https://doi.org/10.1080/25741292.2022.2065065

Freedom House. (2021). *Freedom on the Net 2020: The pandemic's digital shadow*. https://freedomhouse.org/sites/default/files/2020-10/10122020_FOTN2020_Complete_Report_FINAL.pdf

Freedom House. (2022). *Freedom on the Net 2021: The Global Drive to Control Big Tech.* (2022). https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf

Galal, E., & Shehata, M. (2020). Diasporic opposition mediated voices and the digital authoritarianism post the Arab Spring. *Journal of Arab & Muslim Media Research, 13*(1), 3–6. https://doi.org/10.1386/jammr_00007_2

Gao, P., Yu, J., & Lyytinen, K. (2014). Government in standardization in the catching-up context: Case of China's mobile system. *Telecommunications Policy, 38*(2), 200–209. https://doi.org/10.1016/j.telpol.2013.10.002

Ghosh, P. (2021, February 5). Delhi Police write to Google, seek data on toolkit shared by Greta Thunberg. *Hindustan Times*. https://www.hindustantimes.com/india-news/delhi-police-write-to-google-seek-data-on-toolkit-shared-by-greta-thunberg-101612541919875.html

Gillespie, T. (2014). The Relevance of Algorithms. In T. Gillespie, P. J. Boczkowski, & K. A. Foot (Eds.), *Media technologies: Essays on communication, materiality, and society.* The MIT Press.

He, A. (2022). *The Digital Silk Road and China's Influence on Standard Setting.* Centre for International Governance Innovation. https://www.cigionline.org/static/documents/no.264.pdf

Hersey, F. (2022, February 21). *Indian justice proposes police loophole for Aadhaar biometrics access.* Biometric Update. https://www.biometricupdate.com/202202/indian-justice-proposes-police-loophole-for-aadhaar-biometrics-access

Howells, L., & Henry, L. A. (2021). Varieties of Digital Authoritarianism. *Communist and Post-Communist Studies, 54*(4), 1–27. https://doi.org/10.1525/j.postcomstud.2021.54.4.1

Hufbauer, G. & Lu, Z. (2019). *Global e-commerce talks stumble on data issues, privacy, and more* [Policy Brief 19-14]. Peterson Institute of International Economics. https://www.piie.com/sites/default/files/documents/pb19-14.pdf

India bans dozens of Chinese apps after deadly border clash. (2020, June 29). *Global News.* https://globalnews.ca/news/7123461/india-bans-chinese-apps/

Indian government must correct moves toward digital authoritarianism, allow tech platforms to uphold rights. (2021, March 10). Access Now. https://www.accessnow.org/farmer-protests-india-censorship/

Isaac, M. (2021, June 4). WhatsApp Sues India's Government to Stop New Internet Rules. *The New York Times*. https://www.nytimes.com/2021/05/25/technology/whatsapp-india-lawsuit.html

Iyengar, R. (2021, February 10). *Twitter is stuck between a rock and a hard place in India*. CNN. https://www.cnn.com/2021/02/09/tech/twitter-india-government-farmer-protests/index.html

Jamil, S. (2021). The rise of digital authoritarianism: Evolving threats to media and Internet freedoms in Pakistan. World of Media. *Journal of Russian Media and Journalism Studies, 3*(3), 5–33. https://doi.org/10.30547/worldofmedia.3.2021.1

Kemeny, R. (2020, August 19). *Brazil is sliding into techno-authoritarianism.* MIT Technology Review. https://www.technologyreview.com/2020/08/19/1007094/brazil-bolsonaro-data-privacy-cadastro-base/

Khalil, L. (2020, November 2). *Digital authoritarianism: China and COVID.* Lowy Institute. https://www.lowyinstitute.org/publications/digital-authoritarianism-china-and-covid

Kim, M., Lee, H., & Kwak, J. (2020). The changing patterns of China's international standardization in ICT under techno-nationalism: A reflection through 5G standardization. *International Journal of Information Management, 54*, 102145. https://doi.org/10.1016/j.ijinfomgt.2020.102145

KPMG. (2018). *The Changing Landscape of Disruptive Technologies: Tech hubs forging new paths to outpace the competition*. https://assets.kpmg/content/dam/kpmg/it/pdf/2018/04/The-Changing-Landscape-of-Disruptive-Technologies.pdf

KPMG. (2020). *Technology innovation hubs: What technology company executives and venture capitalists should understand about selecting and investing in global technology centers.* https://info.kpmg.us/content/dam/info/en/pdf/2020/tech-innovation-hubs.pdf

Kohno, M. (1995). Ideas and Foreign Policy: The Emergence of Techno-Nationalism in U.S. Policies Toward Japan. In D. P. Rapkin & W. P. Avery (Eds.), *National competitiveness in a global economy* (pp. 199–224). Lynne Rienner Publishers.

Kynge, J. (2020, June 2). *The India-China bust up and what it may mean for tech.* Nikkei Asia. https://asia.nikkei.com/Spotlight/Comment/The-India-China-bust-up-and-what-it-may-mean-for-tech

Lefèvre, F., & Souza, J. (2020, July 8). *Brazil delays privacy law, uses Covid-19 for data grab.* Heinrich Boll Stiftung. https://us.boell.org/en/2020/07/08/brazil-delays-privacy-law-uses-covid-19-data-grab

Lilkov, D. (2020). Made in China: Tackling Digital Authoritarianism. *European View, 19*(1), 110–110. https://doi.org/10.1177/1781685820920121

Mare, A. (2020). State-ordered internet shutdowns and digital authoritarianism in Zimbabwe. *International Journal of Communication*, 4244–2464.

Mari, A. (2019, October 11). *Brazilian government to create single citizen database*. SD Net. https://www.zdnet.com/article/brazilian-government-to-create-single-citizen-database/#:~:text=The%20Brazilian%20government%20will%20create,be%20fully%20shared%20across%20departments

Mihelj, S., & Jiménez-Martínez, C. (2021). Digital nationalism: Understanding the role of digital media in the rise of 'new' nationalism. *Nations and Nationalism, 27*(2), 331–346. https://doi.org/10.1111/nana.12685

Mitra, E., & Hollingsworth, J. (2021, February 3). *India cuts internet around New Delhi as protesting farmers clash with police.* CNN. https://edition.cnn.com/2021/02/01/asia/india-internet-cut-farmers-intl-hnk/index.html

Möllers, N. (2021). Making Digital Territory: Cybersecurity, Techno-nationalism, and the Moral Boundaries of the State. *Science, Technology, & Human Values, 46*(1), 112–138. https://doi.org/10.1177/0162243920904436

Pearce, K. E., & Kendzior, S. (2012). Networked Authoritarianism and Social Media in Azerbaijan. *Journal of Communication, 62*(2), 283–298. https://doi.org/10.1111/j.1460-2466.2012.01633.x

Tiberghien, Y., Luo, D., & Pourmalek, P. (2022). *Existential Gap: Digital/AI Acceleration and the Missing Global Governance Capacity.* Centre for International Governance Innovation. https://www.cigionline.org/articles/existential-gap-digitalai-acceleration-and-the-missing-global-governance-capacity/

Prasad M, D., & Menon C, S. (2020). The personal data protection bill, 2018: India's regulatory journey towards a comprehensive data protection law. *International Journal of Law and Information Technology, 28*(1), 1-19. https://doi.org/10.1093/ijlit/eaaa003

Presidência da República Secretaria-Geral Subchefia para Assuntos Jurídicos. (2018). *LEI No 13.709, DE 14 DE AGOSTO DE 2018.* (2018). http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm

Presidência da República Secretaria-Geral Subchefia para Assuntos Jurídicos. (2019). *DECRETO No 10.046, DE 9 DE OUTUBRO DE 2019.* http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm

Rai, S. (2022, April 13). *India's TikTok Alternative Thrives After Ban on Chinese Apps*. Bloomberg. https://www.bloomberg.com/news/articles/2022-04-13/josh-app-surges-in-india-as-tiktok-replacement

Ricard, J., & Medeiros, J. (2020). Using Misinformation as a Political Weapon:Covid-19 and Bolsonaro in Brazil. *Harvard Kennedy School Misinformation Review.* https://doi.org/10.37016/mr-2020-013

Schneider, F. (2018). *China's digital nationalism*. Oxford University Press.

Sherman, J. (2021). Digital authoritarianism and implications for US national security. *The Cyber Defense Review, 6*(1), 107–118.

Soni, P. (2021, December 14). Online censorship is growing in Modi's India. *Columbia Journalism Review.* https://www.cjr.org/investigation/modi-censorship-india-twitter.php

Sugiyama, S. (2019, June 28). Abe heralds launch of 'osaka track' framework for free cross-border data flow at g20. *Japan Times*. https://www.japantimes.co.jp/news/2019/06/28/national/abe-heralds-launch-osaka-track-framework-free-cross-border-data-flow-g20/

Taliyan, A. (2019, July 4). *G20 Summit: Why India refused to sign Osaka declaration on global data flow.* Times Now News. https://www.timesnownews.com/india/article/g20-summit-why-india-refused-to-sign-osaka-declaration-on-global-data-flow/446887

The Data Protection Bill, 2021. (2021). Trilegal. https://trilegal.com/wp-content/uploads/2021/12/The-Data-Protection-Bill-2021.pdf

The Information Technology Act, 2000, DL-33004/2000. (2000). https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_

updated.pdf

Twitter Safety. (2021, February 10). Updates on our response to blocking orders from the Indian Government. *Twitter*. https://blog.twitter.com/en_in/topics/company/2020/twitters-response-indian-government

Varadarajan, S. (2021, July 18). *Pegasus Project: How Phones of Journalists, Ministers, Activists May Have Been Used to Spy On Them.* The Wire. https://thewire.in/government/project-pegasus-journalists-ministers-activists-phones-spying

Yakovleva, S., & Irion, K. (2020). Pitching trade against privacy: Reconciling EU governance of personal data flows with external trade. *International Data Privacy Law, 10*(3), 201–221. https://doi.org/10.1093/idpl/ipaa003

Yayboke, E., & Brannen, S. (2020). *Promote and Build: A Strategic Approach to Digital Authoritarianism*. Center for Strategic and International Studies. https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism

APPENDIX

TABLE 1. Comparative Look at Mechanisms of Techno-Nationalism and Techno-Authoritarianism in the Context of Datafication

	CONVENTIONAL MECHANISM	WHAT WE OBSERVE IN CONTEXT OF DATAFICATION
Techno-nationalism	Nationalization of digital information infrastructure	Centralized government-led data collection and storage of personal and biometric digital data, creation of "national" databases
	State-led tech innovation and development	Policies that provide domestic firms access to government-collected digital data, with goals of developing domestic tech ecosystems
	Nurturing of domestic tech firms	Data localization policies that protect tech firms from competition, often promoted with nationalist rhetoric
	International expansion of domestic tech firms	
Techno-authoritarianism	Monitoring and surveillance of online activity	Government exemption from digital data protection and privacy laws
	Limiting access to digital information	Regime-led pressure on tech firms to control or limit online discourse, promotion of domestic tech applications
	Censorship and manipulation of public opinion	

Digital Colonialism

Digital Colonialism

AI Diplomacy in National AI Strategies: Addressing Mass Surveillance, Lethal Autonomous Weapons, and Violence from Disinformation in Africa

Bridget Boakye

ABSTRACT:

Like many governments worldwide, policymakers in Africa must address a plethora of complex challenges to harness the potential of AI while governing its responsible use. However, policymakers in Africa are uniquely challenged by the emerging issues of AI governance advanced at the intersection of AI and geopolitics, specifically relating to imported mass surveillance technologies, the use of lethal autonomous weapons developed by foreign actors, and violence from disinformation on foreign-owned social media platforms. These issues disproportionately promulgate harm to the continent and its citizens. This paper presents an overview of the state of AI policy in Africa through a review of the key existing and emerging AI policy initiatives on the continent. To address the three salient AI issues discussed above, the paper examines the importance of national AI strategies and proposes expanding the domains within this instrument to include AI diplomacy, a mechanism to address the impact of harms introduced by technologies developed or imported by foreign countries and companies to Africa.

KEYWORDS: AI in Africa, AI policy in Africa, anticipatory AI policy, AI diplomacy

1 INTRODUCTION

Policymakers around the world now widely accept that artificial intelligence (AI) is not merely an abstract computer domain, but the most transformational technology of our time. However, contrary to the popular belief that Africa is the technological laggard of the world, government digitalization agendas over the last five years and accelerated digitization due to the COVID-19 pandemic are supporting an ongoing expansion of AI in the private and public spheres in Africa (Gehl Sampath, 2021; Ngila, 2022). Emerging evidence points to innovative AI-use cases from agriculture, transportation, and natural language processing in Kenya, Nigeria, Somalia, Ghana, and South Africa, to beneficial AI use in wildlife conservation and point-of-care diagnostics, among others, in Uganda, Ethiopia, and across the continent (Gwagwa et al., 2020).

While the use of AI in Africa has the potential to solve problems, there are also concerns that AI applications introduced by foreign companies and countries are resurfacing, deepening, and introducing new ethical and geopolitical challenges. For example, CNN's report uncovering Russian troll farms in Nigeria and Ghana in 2020 and the exposés revealing the involvement of a data-mining firm, Cambridge Analytica, in Nigeria's and Kenya's elections in 2007 and 2013/2017, respectively, have intensified the local debate on data protection and privacy and have catapulted the role of policy for the AI age in Africa to the international stage (El-Badawy et al., 2021; Boakye, 2021).

Beyond privacy, scholars have identified Africa-specific ethics concerns within the broader ethical AI movement. Concerns about "algorithmic colonialism" and "data colonialism" suggest that the import of Western-developed and/or controlled AI tools to Africa to solve problems is not fit for purpose and often comes at the expense of local solutions, reproducing and reinforcing colonial and neo-colonial power structures (Birhane, 2020; Couldry & Mejias, 2018). The specific threats of imported mass surveillance technologies, lethal autonomous weapons developed by foreign actors, and violence from disinformation on foreign-owned social media platforms are more recent extensions of these ethical concerns.

2 AI POLICY

2.1 DEFINING AI POLICY

AI policy is not often well-defined; definitions are at times in too broad terms, reflecting policies by a myriad of actors on emerging technology, or in too niche terms, relegated to government bans and red lines on AI technologies. In this paper, AI policy refers to three distinct but intersecting areas: direct AI policy, indirect AI policy, and AI-relevant policy (Brundage & Bryson, 2016). Direct AI policies govern AI-based technologies, such as driverless car regulations and AI hiring software. Indirect AI policies such as intellectual property and competition policy laws and startup acts have a broader focus on other technologies or technology in general but affect AI-based technology development. AI-relevant policies, such as education, urban planning, and welfare policies, neither specifically target nor significantly affect AI development but are affected by AI developments (Brundage & Bryson, 2016).

Over the last five years, direct and indirect AI policies have proliferated around the world. The AI policy debate has evolved from whether the government should intervene in AI development and adoption to an acknowledgment that there is a broad range of policies already affecting AI's development and dissemination (Brundage & Bryson, 2016). One indicator, the OECD AI Policy Observatory, the live AI repository of the Organization for Economic Co-operation and Development (OECD), now boasts over 700 policy activities from 60 countries, territories, and the EU, including 251 national AI strategies, agendas, and plans (OECD.ai, 2022).

Noteworthy direct AI policy documents include the European Union (EU) AI Act, which, like EU's General Data Protection Regulation (GDPR), is anticipated by some to become the de facto global AI regulatory tool, delineating risk, responsibilities, rights, and redress for various AI use cases. Policymakers around the world, through their national regulatory bodies, are also developing direct AI policies such as national AI strategies and other indirect AI and AI-relevant policies, e.g., the U.S. Executive Order on Promoting Competition in the American Economy and India's Vision 2030.

2.2 THE IMPORTANCE OF AND ELEMENTS IN NATIONAL AI STRATEGIES

Since the first release by the government of Canada in 2017, national AI policies or strategies have become the most prominent direct AI policy instrument in the world. Adopted by over 44 countries, they have become the standard communication tool of governments' priorities for harnessing AI and their position on the key issues in ethics and governance (Fatima et al., 2021).

The latest data suggests that direct AI policies are important for a country's AI ecosystem, both in its impact on AI-related economic activity and for protecting democratic values, specifically minimizing harm from adopting AI. One prominent index, the Artificial Intelligence and Democratic Values Index by the Center for AI and Digital Policy, shows a clear correlation between national AI strategies and

Direct AI policies are important for a country's AI ecosystem, both in its impact on AI-related economic activity and for protecting democratic values.

progress toward trustworthy AI. The index includes the process of the development of the national AI strategy and its components as key metrics for determining a country's AI and democratic values score (Rotenberg et al., 2022).

While national AI strategies are still fairly nascent, a best practice for this document is beginning to emerge. The World Bank's analytical insights report, "Harnessing Artificial Intelligence for the Development in the Post-Covid-19 Era: A Review of National AI Strategies," highlights eight key policy areas aimed at accelerating AI development and adoption in national AI strategies. They are (1) scientific research, (2) AI talent development, (3) entrepreneurial ecosystem, (4) standards for ethical or trustworthy AI, (5) data access, (6) AI adoption in the public sector, (7) strategic sectoral targeting of AI, and (8) building capabilities of AI governance (World Bank, 2021). Countries currently developing their national AI strategy refer to these policy domains to remain competitive.

2.3 AI POLICY IN AFRICA

AI has been touted by policymakers, industry, and researchers in Africa as a transformative force for African societies, "promising to reduce inequality, alleviate poverty, and improve access to public services like health and education" (Baijnath, 2021). This ambition has been expressed at the highest level of government in various African countries and is beginning to shape policy. In one recent example, Ghana's Vice President, Dr. Mahamudu Bawumia, tweeted on April 28, 2022, "Ghana is now set to move on to the next phase of digitalization with our commitment to build on the current digital platforms and use data analytics and artificial intelligence to provide life-impacting solutions for the ordinary Ghanaian" (Bawumia, 2022).

Beyond the central government, AI policy stakeholders include national and regional bodies such as the African Union (AU), intergovernmental organizations such as the United Nations (UN), and special interest government groups such as the Smart Africa Alliance. Research organizations such as Research ICT Africa and The Future Society also play an increasing role in national and regional AI policy development, providing frameworks and global experience to support the work of African government AI working groups.

At the regional level, the African Union has articulated a strong interest in artificial intelligence, with AI featuring centrally in the AU's Digital Transformation Strategy for Africa (2020-2030). The AU has also established the AU Working Group on AI and is working on the African Union Artificial Intelligence Continent Strategy for Africa, AACS. The Smart Africa Alliance, the multilateral platform for accelerating socio-economic development in Africa through technology, has also launched the African AI Blueprint, a standard framework for national AI strategies on the continent, with objectives to (1) outline the relevant opportunities and challenges of the development and use of AI for Africa and (2) make concrete policy recommendations to harness AI while minimizing its harms (Smart Africa, 2021).

At the national government level, national AI strategies are shaping to become the primary AI policy instruments in many African countries. Two countries, Mauritius and Egypt, have published national AI strategies (OECD.ai, 2022). Mauritius's national AI strategy was produced by senior ministers and advisors in the working group on artificial intelligence, with a focus on matching the potential applications of AI to various areas of the country's economy as aligned with its competitive advantage (Working Group on Artificial Intelligence, 2018). Meanwhile, Egypt's national strategy focuses on harnessing AI to achieve the country's sustainable development goals (National Council for Artificial Intelligence, 2021). Five other African countries are currently developing their national AI strategies, and ten others have instituted AI roadmaps, task forces, and commissions to advance AI policy efforts (Effoduh, 2020).

Other indirect AI and AI-relevant policies primarily concerning digitalization, startups, and data governance also exist in several countries and are regional-level aspirations (Effoduah, 2020). Key AI policy initiatives across Africa and their associated actors are listed in Table 1.

TABLE 1. Key AI Policy Initiatives by Stakeholders in Africa

	ACTORS			
	NATIONAL GOVERNMENTS	**AFRICAN UNION**	**SMART AFRICA**	**UNITED NATIONS (UN)**
Direct AI Policy	Mauritius AI Strategy Egypt AI Strategy	The African Union Artificial Intelligence Continent Strategy For Africa, AACS (~2023)	Blueprint: Artificial Intelligence for Africa	UNESCO Recommendation on Ethics of AI
Indirect AI Policy	Malabo Convention Data Protection Regulation National Digital Strategies (e.g., Nigeria Digital Economy & Strategy 2019, Kenya Digital Economy 2019, Digital Senegal 2025) Startup Acts (e.g., Tunisia Startup Act, Senegal Startup Act)	Digital Transformation Strategy for Africa Africa Data Policy Framework (~2023)	N/A	N/A
AI-Relevant Policy	Ghana Free SHS Policy, 2017	Africa Continental Free Trade Area (AfCFTA) Agreement Agenda 2063	N/A	N/A

Finally, international AI policy instruments also play a role in Africa's AI policy landscape. The Recommendation on Ethics of AI by the United Nations Educational, Scientific and Cultural Organization (UNESCO) was signed by all African UNESCO member countries and provides common values and principles on the ethics of AI. While nonbinding, the Recommendation sets a global normative framework for protecting and promoting human rights and the environment with AI, including practices that countries can apply through their policy and legal instruments.

3 AI & GEOPOLITICS

3.1 EMERGING ISSUES IN AI & GEOPOLITICS IN AFRICA

Governments are beginning to view the challenges of AI more broadly. Concerns about the technology have moved from abstract fears about "robot takeovers" to urgent questions on national and international security, social and radical justice, safety, research and development, labor and the economy, and more (McAllister, 2020).

While these issues affect all countries to a degree, they are more urgently relevant for Africa, moving beyond salient questions to lived reality, first or disproportionately impacting the continent and its citizens. The issues of imported mass surveillance technologies, lethal autonomous weapons developed by foreign actors, and violence from disinformation on foreign-owned social media platforms are surfacing in many countries in Africa, but their presence and impact have not been well documented, except in a few country-specific cases. The case studies below highlight three recent and primary cases of each issue and their impact.

3.2 CASE STUDY: FOREIGN IMPORTED MASS SURVEILLANCE TECHNOLOGIES, SOUTH AFRICA

Mass surveillance has become one of the most contentious issues in the global public debate on AI. For many foreign companies, Africa represents a high-growth market given both private and public interest in surveillance. The continent also represents a place to perfect these technologies given nonexistent or lax regulation. Research suggests that mass surveillance technologies developed in the West are often imported to and tested in African countries, where they have significant social and economic impacts. South Africa is of particular concern.

In a 2022 *MIT Review* investigative piece on digital mass surveillance in South Africa, Kyle Dicks, a Johannesburg-based sales engineer for Axis Communications, revealed that when AI is "...developed in Europe and America and all of these places … often South Africa is the place to put them to the test" (Hao & Swart, 2022). Activists say that these imported technologies are "fuelling a digital apartheid where cameras have re-created the digital equivalent of passbooks, the apartheid-era system that the government used to limit Black people's physical movements in white enclaves." This use of surveillance technologies to monitor the movements of Black people in South Africa threatens not only people's democratic freedoms but also their economic well-being. As the piece explains, the privatization of security is taking priority over social welfare programs in addressing social ills (Kao & Swart, 2022). Other African countries such as Kenya, Botswana, and Ivory Coast are also embarking on safe city initiatives, with activists documenting similar concerns (Mudongo, 2021).

3.3 CASE STUDY: LETHAL AUTONOMOUS WEAPONS (LAWS), LIBYA

In early 2021, the United Nations (UN) Security Council published a report that the lethal autonomous weapons used in Libya were used to target people. The report stated that military convoys were "hunted down and remotely engaged by the unmanned combat aerial vehicles or the lethal autonomous weapons systems … The lethal autonomous weapons systems were programmed to attack targets without requiring data connectivity between the operator and the munition: in effect, a true 'fire, forget and find' capability" (United Nations, 2021). While drone warfare is not new, the Libya case, if confirmed, would be the first use of "a killer drone with a mind of its own." The UN, through the Convention on Certain Conventional Weapons, holds exclusive authority over decisions on LAWs. However, the immediate and life-threatening implications of the AI arms race for the availability and use of LAWs in Africa means that African governments should further probe foreign stakeholders on their development and import of LAWs in their current policy deliberations.

3.4 CASE STUDY: VIOLENCE FROM DISINFORMATION, ETHIOPIA

In late 2021, several media organizations in the United States published the "Facebook Papers," detailed internal

Facebook research about the negative impacts of many of its products on society. In addition to other harms, the papers revealed Facebook's repeated content moderation failures in Ethiopia and, specifically, the ties between the call to violence on social media and real-world/offline violence during the Ethiopian civil war (Guest & Zelalem, 2021).

According to internal documents, Facebook's tier system for prioritizing content moderation resources, including its content moderation algorithms, is a symptom of deep geographic and linguistic inequality toward non-English-speaking countries (Mackintosh, 2021). But while federal inquiries were held in the U.S., the U.K., and EU parliaments with whistleblower Francis Haugen, there were none in Africa. Although the impact of the harms on the platform was global, African governments had no response to the Papers. They did not demand rectification from Facebook, as was the case for other governments in the West (Rest of World, 2021).

4 RECOMMENDATIONS

As the case studies above illustrate, the issues of imported mass surveillance technologies, the use of lethal autonomous weapons developed by foreign actors, and violence from disinformation on foreign-owned social media platforms show early or disproportionate impacts on Africa. These issues will likely compound and worsen with time if not addressed promptly and in cooperation with international governments and companies. This paper proposes that national AI strategies could be the solution, with AI diplomacy being the specific mechanism.

4.1 THE POTENTIAL FOR NATIONAL AI STRATEGIES TO ADDRESS AI HARMS

This paper discusses issues at the intersection of AI and geopolitics and new policy instruments such as "tech-forward foreign policies" that have the potential to address these issues (Erzse & Garson, 2022). "Tech-forward foreign policies" are coherent government strategies that address the impact of technology on intercountry power relations. These policies further the idea of global cooperation through diplomacy as key to addressing complex technology policy issues.

"Tech-forward foreign policies" are, however, yet to gain traction in Africa given the challenges of designing and implementing them. These challenges include a lack of resources (financial, human, and technical) for technology policy, political instability in some countries, insufficient infrastructure, and other pressing issues such as poverty, healthcare improvement, and national security.

But a lack of resources does not mean that the issues of imported mass surveillance technologies, use of lethal autonomous weapons, and violence from disinformation on social media should go unaddressed. National AI strategies are a key AI policy document with great interest across the continent. Embedding elements of "tech-forward foreign policy," specifically the concept of AI diplomacy, as a unique domain within national AI strategies can be a meaningful short- to medium-term solution to these AI harms. The concept of AI diplomacy involves addressing the challenges introduced by the influence and impact of AI-related activities by foreign countries and companies.

AI diplomacy involves addressing the challenges introduced by the influence and impact of AI-related activities by foreign countries and companies.

In advancing AI diplomacy, African policymakers should:

1. *Institute a Ministerial Committee to oversee smart/safe city initiatives.*

There are currently eight African countries with government facial recognition projects, seven with smart/safe city initiatives, and six with smart policing initiatives, most of which require procurement of foreign technologies (Mudongo, 2021). To address the challenges introduced by this ***import of mass surveillance technologies***, governments should institute a Ministerial Committee of the relevant ministers (for example, the Minister of Digital Economy, the Minister of Public Services, and the Minister of National Security) to oversee all smart/safe city initiatives where they exist or are being considered. A country's data protection commissioner, where one exists, should also be a member. While African governments work on developing and enforcing legal instruments on data protection and privacy, this Ministerial Committee can act as the responsible owner of smart/safe city initiatives to ensure they are implemented effectively and safely. Singapore, which has won worldwide acclaim for its smart nation initiative, has such an oversight Ministerial Committee (Smart Nation Platform Solutions Group, 2019).

2. *Make the country's stance on LAWs explicit in national AI strategies and connect the role of the data protection commissioner with that of the interior minister.*

To address the pressing concern of the ***use of Lethal Autonomous Weapons***, African governments should make explicit their stance on LAWs in the AI diplomacy domain of their national AI strategies and connect the role of the data protection commissioner, who often oversees AI strategy, with the interior minister, who oversees internal security in a country. This direct relationship can be helpful for knowledge transfer and intelligence sharing while building a country's position that can be advanced at the pan-African and global levels. Countries such as Ghana have already shown leadership in this realm. Supported by Sierra Leone, South Africa, Uganda, Zambia, and Zimbabwe, Ghana, as well as some non-African states, expressed a desire to negotiate a new international treaty on lethal autonomous weapons (Effoduh, 2020).

3. *Explore the role of tech ambassadors to social media companies.*

To address the issue of ***violence from disinformation on social media,*** African governments should explore the role of tech ambassadors to major social media companies as part of a bouquet of efforts in AI diplomacy to build relationships with industry and ensure they act responsibly (Erzse & Garson, 2022). Tech ambassadors can ensure that firms aren't held accountable only to richer countries but apply equitable resources to address harms across the board.

5 CONCLUSION

Many times, activists fear that Africa's response to harms perpetrated against its environment and people come too late. Through the instrument of national AI strategies, African policymakers do not have to miss the critical window of opportunity to address the issues of the import of mass surveillance technologies, the use of lethal autonomous weapons developed by foreign actors, and violence from disinformation on foreign-owned social media that are beginning to promulgate harms on the continent. National AI strategies are already of interest to countless governments across the continent who hope it will help them advance AI development and deployment to address critical issues. By advancing the concept of AI diplomacy as a unique domain within national AI strategies through the specific recommendations above, policymakers can ensure they have a timely response to the complex challenges their countries face at the intersection of AI and geopolitics.

REFERENCES

Baijnath, M. (2021, May 19). *The Growth of Artificial Intelligence in Africa: On Diversity and Representation.* IRCAI. https://ircai.org/the-growth-of-artificial-intelligence-in-africa-on-diversity-and-representation/#:~:text=AI%20is%20poised%20to%20impact

Bawumia, M. [@MBawumia]. (2022, April 28). I noted that Ghana is now set to move on to the next phase of digitalization with our commitment [Tweet]. Twitter. https://twitter.com/MBawumia/status/1519618672083574787

Birhane, A. (2020). Algorithmic colonization of Africa. *SCRIPT-ed 17*(2), 389-409.

Boakye, B. (2021, July 1). *Tech Policy in Africa: Emerging Trends in Internet Law and Policy.* Tony Blair Institute for Global Change. https://institute.global/policy/tech-policy-africa-emerging-trends-internet-law-and-policy

Boakye, B., Furlong, P., Zanderman, K. (2022). *Repairing the Rewards of the Next Technological Revolution: How Africa Can Accelerate AI Adoption Today.* Tony Blair Institute for Global Change. https://institute.global/policy/reaping-rewards-next-technological-revolution-how-africa-can-accelerate-ai-adoption-today

Brundage, M. & Bryson, J. (2016). Smart Policies for Artificial Intelligence. ArXiv:1608.08196 [Cs]. https://arxiv.org/abs/1608.08196

Couldry, N. & Mejias, U.A. (2018). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, *20*(4):336-349.

Effoduh, J. O. (2020). *7 Ways that African States are Legitimizing Artificial Intelligence*. Open AIR. Retrieved March 15, 2022, from https://openair.africa/7-ways-that-african-states-are-legitimizing-artificial-intelligence/

El-Badawy, E., Munasinghe, S., Bukarti, A. B., & Bianchi, B. (2022, March 1). *Security, Soft Power and Regime Support: Spheres of Russian Influence in Africa*. Tony Blair Institute of Global Change. https://institute.global/policy/security-soft-power-and-regime-support-spheres-russian-influence-africa

Erzse, A. & Garson, M. (2022). *A Leader's Guide for Building a Tech-Forward Foreign Policy.* Tony Blair Institute for Global Change. Available from https://institute.global/policy/leaders-guide-building-tech-forward-foreign-policy

Fatima, S., Dawson, G., Desouza, K., & Denford, J. (2021). *Winners and losers in the fulfillment of national artificial intelligence aspirations.* Brookings. https://www.brookings.edu/blog/techtank/2021/10/21/winners-and-losers-in-the-fulfilment-of-national-artificial-intelligence-aspirations/#:~:text=Clearly%2C%20having%20a%20national%20AI

Gehl Sampath, P. (2021). *Governing artificial intelligence in an age of inequality.* Global Policy, 12(56), 21- 31.

Guest, P. and Zelalem, Z. (2021, November 13) *Why Facebook keeps failing in Ethiopia*. Rest of World. Retrieved June 1, 2022, from https://restofworld.org/2021/why-facebook-keeps-failing-in-ethiopia./

Gwagwa, A., Kraemer-Mbula, E., Rizk, N., Rutenberg, I., & De Beer, J. (2020). Artificial intelligence (AI) deployments in Africa: Benefits, challenges and policy dimensions. *The African Journal of Information and Communication (AJIC), 26*, 1-28. https://doi.

org/10.23962/10539/30361. [Accessed 15 March 2022]

Hao, K. & Swart, H. (2022, April 19). *South Africa's Private Surveillance Machine is Fueling a Digital Apartheid*. MIT Technology Review. Retrieved April 19, 2022, from https://www.technologyreview.com/2022/04/19/1049996/south-africa-ai-surveillance-digital-apartheid/

Mackintosh, E. (2021, October 25). Facebook knew it was being used to incite violence in Ethiopia. It did little to stop the spread, documents show. CNN. https://www.cnn.com/2021/10/25/business/ethiopia-violence-facebook-papers-cmd-intl/index.html

McAllister, K. (2020). *The questions the candidates should answer on AI policy*. Protocol. https://www.protocol.com/ai-policy-questions-presidential-candidates?rebelltitem=2#rebelltitem2

National Council for Artificial Intelligence. (2021). *Egypt National Artificial Intelligence Strategy.* Ministry of Communications and Information Technology. https://mcit.gov.eg/Upcont/Documents/Publications_672021000_Egypt-National-AI-Strategy-English.pdf

Mudongo, O. (2021, January). *Africa's Expansion of AI Surveillance — Regional Gaps and Key Trends. Research*. ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2021/01/AI-Surveillance_Policy-Brief_Oarabile_Final.pdf

Ngila, F. (2022, June 23). *Africa is Going Big on AI. Quartz*. Retrieved April 19, 2022, from https://qz.com/africa/2180864/africa-does-not-want-to-be-left-behind-in-the-ai-revolution/

Oecd.ai. (2022). *OECD AI live repository of over 260 AI strategies & policies - OECD.AI*. Retrieved June 30, 2022, from https://oecd.ai/dashboards

Rest of World Staff (2021). *Why the rest of the world shrugged at the Facebook Papers*. Rest of World. https://restofworld.org/2021/rest-of-the-world-reaction-facebook-papers/.

Rotenberg, M., Hickok, M., Caunes, K. (Eds.). (2022). *Artificial Intelligence and Democratic Values Index*. Center for AI and Digital Policy. https://www.caidp.org/reports/aidv-2021/

Smart Africa Alliance. ***Artificial Intelligence for Africa Blueprint.*** (2021). https://smart.africa/board/login/uploads/70029-eng_ai-for-africa-blueprint.pdf

Smart Nation Platform Solutions Group. (2019). GovTech Singapore. Available from: https://www.w3.org/WoT/ws-2019/Presentations%20-%20Day%202/02_W3C%20WOT%20FINAL.pdf. [Accessed 1 November 2022]

United Nations Security Council. (2021). Letter dated 8 March 2021 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council. S/2021/229. Retrieved April 19, 2022, from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/037/72/PDF/N2103772.pdf?OpenElement

Working Group on Artificial Intelligence. (2018). *Mauritius Artificial Intelligence Strategy.* National Computer Board. https://ncb.govmu.org/ncb/strategicplans/MauritiusAIStrategy2018.pdf

World Bank Group (2021). *Harnessing Artificial Intelligence For Development in the Post-Covid-19 Era: A Review of National AI Strategies and Policies.* https://thedocs.worldbank.org/en/doc/2e658ef2144a05f30e254221ccaf7a42-0200022021/original/DD-Analytical-Insights-Note-4.pdf

The Impact of New Technology

Acquisition and Use of Smart City Technologies in Africa: Patterns and Implications

Cecil Abungu and Adi Guyo

ABSTRACT:

Technologies that make a city “smart” have long been sold as the solution to the burgeoning challenges that come with urban sprawl across the world. The narrative seems to have been successful in a range of African countries as well, where smart city technologies are being acquired and used at a surprisingly brisk pace. In this paper, the authors examine all African smart city technology acquisition deals that are publicly available. They also assess the uses to which the technologies are put, all with the aim of finding any major patterns and then identifying the democratic and geopolitical implications. The inquiry finds that the acquisition and use of these technologies creates a raft of democratic concerns that need to be addressed urgently. As for geopolitical patterns, it finds that the longstanding narrative of China as the dominant player in this market is not entirely accurate. A critical mass of Western entities are also supplying these technologies in smart city-oriented African countries in the same ways that Chinese entities have done.

KEYWORDS: Africa, smart city, smart city technologies, acquisition, use, democracy, geopolitics, China, Western

1 INTRODUCTION

Smart cities have been broadly defined as cities that “use information and communication technologies (ICT) to be more intelligent and efficient in the use of resources, resulting in cost and energy savings, improved service delivery and quality of life, and reduced environmental footprint—all supporting innovation and the low-carbon economy” (Parvez, 2016, p. 178). The main goals of a smart city seem to be to optimize city functions, promote economic growth, and improve the quality of life for citizens by using technologies, tools, and data analysis (TWI Global, n.d.).

The most important driver of smart cities is the development and use of technologies such as artificial intelligence, geospatial technology, the Internet of Things (IoT), and 5G networks. Artificial intelligence (AI) is technology in which algorithms are used to find patterns in a vast amount of data and thereafter make predictions, recommendations, and decisions (Swejis et al., 2017, p. 28). The development and use of AI has been instrumental to smart cities in many ways. For

The Impact of

example, it has been used to manage security through city surveillance (Feldstein, 2019), and law enforcement officials use patterns it extracts from existing data to decide where (or on whom) to focus their attention (Schwab, 2017). It has also been used to control pollution, transport, and mobility in a city (Berry, 2021).

Geospatial technology (the collection of location-specific data) is crucial to the efficiencies of smart cities, since the use of Geographic Information System (GIS), Remote Sensing (RS) and Global Positioning System (GPS) enables the acquisition of data on the earth that is used for analysis ("What is Geospatial Technology," 2018). Smart cities would not be possible without IoT technology, which allows the various technologies to "speak to each other." For example, sensors collect data on whether there are people or cars on a street and, through IoT, activate or deactivate the street lights. The technology has also made it possible for city administrators to improve managing waste disposal, parking spots, and traffic flow. Finally, the 5G network makes it possible for data to be transferred incredibly fast between domains.

In this paper, we assess some African governments' acquisition and use of such technologies in the context of smart cities. In particular, we focus on how their acquisition and deployment is (or is likely to) impact freedom and democracy. We use here Friedrich Hayek's conception of freedom as the condition of people in which coercion of some by others is reduced as much as possible in a society (1960, p. 11), understood alongside Elizabeth Anderson's definition of freedom as the sociologically complex condition of nondomination (Anderson, 2018, p. 4). As for democracy, we take K. Sabeel Rahman and Hollie Russon Gilman's understanding that it requires citizens' meaningful participation in decisions that impact their lives. This necessitates that the power hierarchy between a state and its citizens is not substantially warped (Rahman & Gilman, 2019, p. 113).

Our main findings are as follows. First, the oft-repeated claim that Chinese companies dominate the sector does not match the evidence available. Several other companies from the West and the Middle East have won important contracts. Even for security-related technologies, the acquisition and use of technologies made by Chinese entities is not so obviously prioritized. It is only in the supply of 5G technologies that China-based Huawei seems to entirely dominate. Second, the acquisition of these technologies by African governments features a significant degree of opacity, a development that is worrisome for democracy. Third, the use of technologies unrelated to security is generally benign and seems to have improved the quality of life for people in urban centers. It is the use of security-related technologies that has been worrisome. It has enabled the consolidation of power by political elites in Africa, and has created an avenue through which they can chill democratic speech. Finally, we call for increased focus on the governance of acquisition and use of smart city technology in African countries.

Security-related technolog[y] ... has enabled the consolidation of power by political elites in Africa, and has created an avenue through which they can chill democratic speech.

2 ACQUISITION OF SMART CITY TECHNOLOGIES IN AFRICA

This section will discuss the various smart city technologies used around the continent, with a focus on which entities are contracted to supply them.

2.1 DATA CENTERS AND DATA PLATFORMS

A data center is a site hosting all necessary systems for the operation of IT applications ("Cloud computing in Africa," 2021, p. 15). It has three fundamental components: the infrastructure, which comprises the equipment needed to support its operations (power transformers, power supplies, generators, air-conditioning units, power distribution systems, etc.), the IT equipment (servers, system management tools, and network equipment), and the operating areas for the staff ("Cloud computing in Africa," 2021, p. 16). The following are some data centers and platform deals that are worth noting.

In Egypt, the government has sought to build 38 new smart cities across the country in order to introduce the use of AI and technology in line with Egypt's sustainable strategy ("Why the government is moving towards smart cities," 2022). The UAE's state-owned company Etisalat Misr will be working on data centers that will monitor all the smart systems in the smart cities ("Honeywell, Etisalat Misr, ACUD to deploy tech," 2020).

In the same vein, Konza is a smart city in Kenya whose construction was launched in 2008 as part of the country's Vision 2030 (Baraka, 2021). As part of its development, the Konza Technopolis Development Authority (KoTDA) entered into an agreement with Huawei to build a data center through Chinese concessional loans (Moss, 2019).

The same trend can be seen in Casablanca, where Minsait was awarded the contract to develop a smart city that would serve as a model for the urban modernization of Morocco (Minsait, 2019). More specifically, the company is expected to develop an urban data platform in order to increase the efficiency of services, waste collection, slaughterhouse management, and wholesale markets, and to improve the quality of life and promotion of transparency (Minsait, 2019). Minsait, whose parent company is Indra Sistemas, is a publicly listed company on the Madrid Stock exchange ("Share price and profitability of the share Indra Sistemas," n.d.). There is no list of shareholders online, which makes it difficult to determine whether a foreign government may have a significant influence on its dealings ("Shareholder Structure," n.d.). The government of South Africa has also contracted Huawei to put in place a cloud-based data center to improve government efficiency by integrating the diverse government applications and ensuring its security (Huawei, n.d.).

Despite their benefits, data centers may suffer from potential internal or external risks. Internal risks can be human error, technical component malfunctions, and architecture failure. External risks are sabotage, internet connectivity issues, and failure in the power supply network ("Cloud computing in Africa," 2012, p. 17). Data centers may use cloud computing that poses security challenges for data privacy, data integrity, data loss or leakage, a malicious insider, and IP spoofing (Monika, 2017, p. 5; Sun et al., 2014, pp. 3,6).

2.2 INFRASTRUCTURE FOR WIRELESS NETWORKS

Wireless networks transmit and receive data using radio waves ("Securing your wireless network," n.d.). They offer advantages compared to wired alternatives (Ahmad, 2009, p. 19). However, security concerns arise from misconfiguration or incomplete configurations, denial of service, passive capturing (eavesdropping), rogue/unauthorized/ad hoc access points, evil-twin attacks, and hacked lost or stolen wireless devices (Wilkins, 2011; CISA, 2018; Froehlich, 2021). Again, there are deals worth highlighting, as follows.

In Ghana, the National Communications Authority granted state-owned Celltel the contract to provide households and institutions with consistent and reliable wi-fi connectivity through the Ghana Smart City Project (O'Grady, 2022). The company noted that it would use a mixture of Chinese and U.S. technology. Device parts would be manufactured by China's Hi-Tech Company, a subsidiary of Electronic Conglomerate Haier, and Cisco, which would make routers and networking gear (Olander, 2022). Since Hi-Tech Company is state owned (Sovereign Wealth Fund Institute, n.d.), there is every reason to believe that this deal had the direct backing of the Chinese government. On the other hand, Cisco is an American company publicly traded on the

stock market (Cisco, 2017), and there are no signs of any state influence on the company.

In South Africa, the smart city of Ekurhuleni has cooperated with Huawei to deploy a city-wide wired and wireless network to provide free, public wi-fi (Huawei, n.d.). Huawei has also partnered with various companies in Africa to supply the infrastructure for their 5G networks. These partnerships include MTN in Zambia ("China helps advance technology in Africa," 2022), Ethio in Ethiopia ("Ethio Telecom to Pilot 5G Network in Ethiopia," 2021), Rain in South Africa (Tomás, 2019), and Safaricom in Kenya (Idris, 2021).

2.3 TRANSPORT AND MOBILITY TOOLS

Some technological tools are built to enhance the ease with which people move around a city. One good example is the Ethiopian government's contract with Dayang Auto-Parking Equipment Co Ltd, a Chinese smart-parking manufacturing company. The company has been hired to construct a smart-parking project, together with a local electromechanical works contractor, SYSPROEN Systems and Engineering Ltd (Oirere, 2019). It is not clear who brokered the deal, as information about the negotiation process is not available to the public.

2.4 TOOLS FOR ENHANCING SECURITY

African governments have been very active in acquiring security-related technologies, and in this regard, there is a litany of examples one can focus on. In Egypt, the local government contracted Honeywell to install 6,000 security cameras across a secure wireless network in the new capital ("Honeywell, Etisalat Misr, ACUD to deploy tech," 2020). In the first phase of the development, Elsewedy Electric and two unnamed Chinese and French companies won a tender to supply 200,000 smart meters ("Why the government is moving towards smart cities," 2022). Honeywell is a publicly traded American multinational conglomerate corporation (Honeywell, n.d.), while partner group Etisalat Misr is a subsidiary of Etisalat Group ("Honeywell, Etisalat Misr, ACUD to deploy tech," 2020). Only 40% of the company is traded publicly, while the rest of the shares are owned by the UAE government, which, as the majority shareholder, is likely to influence company dealings (Etisalat, n.d.). On the other hand, Elsewedy Electric is an Egyptian multinational electrical company that has been listed on the Cairo stock exchange since 2006 (Elsewedy Electric, n.d.). As such, it is not likely to have foreign government influence.

In Morocco, the Dakhla smart city's determination to have more secure streets has led it to collaborate with Huawei (Rahhou, 2021; "Cooperation between Wilaya Von Dakhla and Huawei." 2021). The cooperation will facilitate the deployment of intelligent video-protection systems to strengthen security in the city, as well as to focus on areas such as education, health, and renewable energy ("The Wilaya of Dakhla and Huawei," 2021).

Additionally, Zimbabwe has partnered with Huawei and CloudWalk (both are Chinese companies) to supply it with surveillance systems for law enforcement (Privacy International, 2021). Huawei received $20 million to start the installation of a grid of public surveillance cameras as part of a smart city project, while CloudWalk would supply facial recognition technology (Privacy International, 2021). CloudWalk would commence a large-scale facial recognition program by using photographs to train its systems to identify different ethnicities (Chimhangwa, 2020; Gallagher, 2019, p. 35). China partnered with Zimbabwe in part to speed up their algorithm training for diversity (Chimhangwa, 2020).

East African countries have not been left behind. In 2019, Uganda invested $126 million to acquire surveillance technology from Huawei (Jili, 2020a). This led to concerns that its use would instead be diverted to track government critics. True to that, singer and opposition leader Bobi Wine's encrypted communication was intercepted.

The spread of surveillance technology without adequate checks in Africa is reshaping governance, as it can potentially be used as a tool of repression (Jili, 2020a). Another surveillance concern across the continent is the practice of remote hacking that enables governments to access files on a target laptop. Webcams and microphones can also be accessed in the process (Jili, 2020a).

2.5 TOOLS FOR PERFORMING A WIDE RANGE OF URBAN SERVICES

The Internet of Things (IoT) technology enables the implementation of systems interconnecting several objects in either the physical or the virtual world. Many sensor tools adopted IoT technology for data collection. This may cause security concerns in the form of Denial-of-Service attacks, replay attacks, password-guessing attacks, and IP-spoofing attacks (Azrour et al., 2021).

The Honeywell–Etisalat Misr deal in Egypt is an excellent example. Honeywell was contracted to develop a citywide IoT platform that would include a management dashboard, smart city services, a citizen engagement portal, and mobile application capabilities in the new capital. The use of the technology is expected to reduce waste and to manage transportation systems and smart parking to support sustainability efforts ("Why the government is moving towards smart cities," 2022). Nokia has also entered into a contract with the government of Rwanda to provide it with a wide range of smart city technologies, including network connectivity and sensor tools that are meant to improve areas such as public safety, waste management, and healthcare (Nokia, 2017).

One final example is the Mohammed VI Tangier Tech City, a joint project between the Moroccan and Chinese governments. Contracts for the technological tools that will power the city are almost entirely going to Chinese entities ("Large-scale infrastructure projects in Tangiers," n.d.). The China Communication Construction Company and its subsidiary China Road and Bridge Corporation—which is fully owned by the Chinese government—hold the contract. The companies' success in getting the contracts is likely to have been influenced by the role they play in the Belt and Road Initiative, which has also influenced the development of this smart city (Hamama, 2020).

2.6 PATTERNS OBSERVED IN ACQUISITION

Generally, there is little transparency in the acquisition process of smart city technologies. Citizens are often only made aware of it at the implementation stage, not the negotiation stage. There is little to no public explanation of why the technologies are acquired. This is deeply concerning for democracy, since it means that citizens are completely cut out of a crucial part of the move toward smart cities.

The common narrative that Chinese companies dominate smart city technology in Africa is not entirely accurate.

Our research shows that the common narrative that Chinese companies dominate smart city technology in Africa is not entirely accurate (Deutsche Welle, n.d.-b). It seems true that Huawei and other Chinese companies have won most of the contracts to supply 5G infrastructure and security-related smart city technologies. Nevertheless, it is definitely not the only important player. As demonstrated earlier in this paper, companies from the United States and the UAE are also receiving some of the contracts. In fact, other than security-related tools, it appears that there are a number of non-Chinese companies winning contracts.

Occasionally, it is possible to infer a foreign company's strong involvement in the negotiation. Even then, there is no real reason to find some common narratives about the involvement convincing. For example, the claim by the U.S.-China Security Review Commission that China sees the export of its technologies as a way to embed its model of governance in developing countries (Green et al., 2020, p. 3) seems speculative relative to the evidence available. There is a strong case to be made that China simply sees African smart cities as good markets for its products, especially because of the weak regulation of personal data (which can

be used to train algorithms developed in China) (Hawkins, 2018).

Finally, it appears that where local African companies are contracted, they still end up subcontracting foreign companies from countries such as the United States and China to supply the core technological tools.

3 PATTERNS AND IMPLICATIONS OF THE USE OF SMART CITY TECHNOLOGIES

Our study sought to discover any patterns and implications of the use of smart city technologies in Africa. "Use" here is considered in the context of not only how the African governments have used the technology but also other influences that may be observed because of the technology.

On close examination, it appears that the non-security-related technological tools have generally made life better for many citizens on the continent (Kimuyu, 2021). The greatest worry for freedom and democracy on the continent comes from the security-related tools.

Non-security-related [smart] technological tools have generally made life better for many citizens on the continent. The greatest worry for freedom and democracy … comes from the security-related tools.

As has been observed by Woodhams (2020), security-related technologies in the field are often used beyond what they were disclosed to do. The communicated motivation for acquiring the technologies is usually to increase security in a particular place. Do they meet this goal? There is some evidence from Kenya, where the National Police Service reported only marginal reduction in crime detection after using Huawei's technologies (Crime Statistics, n.d.).

More concerningly, the technologies are regularly used beyond what was intended. For example, surveillance technologies that were initially supposed to enhance security are often used to infringe on privacy. In Uganda, the surveillance technology purchased in 2019 has presented democratic challenges. Surveillance techniques such as remote-hacking and eavesdropping (Jili, 2020b) are used to aid in political intimidation. The protection of location privacy is also becoming increasingly more difficult as the number of CCTVs continue to rise. This has a negative effect on democratic life, as people are less likely to participate if they feel that they are being watched and their every move tracked (Duncan, 2018).

In Zimbabwe, as part of the voter registration process before the 2018 elections, the government began collecting citizens' biometric data. Information such as national identity numbers, home addresses, fingerprints, and photos were integrated into a digitized system. The citizens were fearful that it would be an avenue for monitoring and political intimidation (Chimhangwa, 2020).

In places like Zambia, Uganda, and Nigeria, such misuse is often aimed at reining in political rivals. According to a Wall Street Journal investigation, Huawei employees were found to have helped Ugandan and Zambian governments spy on their political opponents (Feiner, 2019). There are, however, two interesting points to note. First, the employees in question apparently acted on behalf of the specific African government and not for the Chinese government. Second, the investigation "did not find any unique features in Huawei's technology that allowed spying activity to occur." Instead, the Huawei technicians working in Uganda's police headquarters used "Pegasus-style spyware created by unknown parties" (Feiner, 2019). However, technological

tools built by Huawei in the past have also been customized specifically to allow for such use (Deutsche Welle, n.d.-a). Huawei has a potentially negative impact on a country's security. Some equipment could have been manufactured in a manner that allows vulnerability for cyberattacks for the military and industrial espionage. Sensitive information could also be exposed to theft (Deutsche Welle, n.d.-a).

People's and groups' ability to exercise their civic freedoms and challenge positions taken by important players also depends on the contexts in which they find themselves. It is clear that these security-related smart city technology tools have created a new avenue for powerful players in governments around Africa to increase their power and chill speech. This is a concerning development for those who believe in freedom and democracy. The risk of what has been referred to as "neo-digital colonialism" (Gravett, 2020, pp. 126–7) is also very real. Using tools designed by entities that are at the beck and call of foreign governments is not a trustworthy way to protect one's sovereignty.

4 RECOMMENDATIONS

In light of the foregoing assessments, policymakers in African countries should take a few steps in the acquisition and use of technology for their cities.

1. *Careful auditing of technologies and tools already in use.*

   As discussed in the preceding parts of this paper, there are already several technologies and tools that have been acquired and are used in African cities. The first step that policymakers ought to take is a detailed and rigorous audit reviewing (1) whether these technologies should continue to be used and (2) whether the tools that use those technologies are the most appropriate ones. Several considerations should be made under such a review, including how expensive it is to use the tools, how easily they can be misused, and whether—in their use so far—they have been meeting the goals for which they were acquired. Such an audit should be followed by decisions on which technologies and tools are worth preserving and which ones ought to be eliminated.

2. *More consultative processes to determine which technologies and tools are necessary.*

   It would also be important for policymakers to have in place more consultative and participative processes in decision-making about which technologies should be acquired and which tools should be used. Our research has shown that these decisions are currently made in an opaque manner, and often citizens and nonprofits are only able to make their voice heard after the technologies are already in use. This is unfortunate, especially because several of the countries studied claim that democracy is a prized value. Having more consultative processes in place will allow for more buy-in, and could also go a long way to prevent endless and antagonistic litigation in domestic courts.

3. *More transparent processes for acquisition of the agreed-upon technologies and tools.*

   Similarly, the processes for acquiring these technologies and tools need to be more transparent than they currently are. Our research has demonstrated that in many of these countries the tenders are closed or the specific reasons contracts are granted to certain entities are undisclosed. These unknowns have created a perfect breeding ground for corruption and backdoor dealing, where those in charge are able to award contracts to entities that assure them of control over these technologies and tools. This can be corrected if transparency is taken more seriously in the acquisition processes.

4. *Vigorous public education on why the relevant technologies and tools are in use.*

   It is not enough to create participative frameworks for determining which technologies and tools are useful. It is also important for policymakers and civil society to take seriously their duty to educate people on what these technologies and tools are used for as well as what they can and cannot do according to the law. Not only will this step empower citizens, it will also

create the conditions to give more legitimacy to such decisions.

5. *A more serious and evidence-based approach to the "China-is-dominant" narrative.*

   As we have shown in the preceding parts of this paper, the idea that China is the dominant actor from whom city technology tools are acquired is not entirely backed by the available evidence. It is important that African governments correct this narrative by referring to existing evidence and available data, since (1) the claim is inaccurate, and (2) the claim usually ends up fraying geopolitical ties, which impacts the possibility of cooperation between African and Western countries like the United States in sharing technology and intelligence.

5 CONCLUSION

Smart city technologies can be a critical driver of better-managed urban spaces, where citizens enjoy a high quality of life alongside all the perks of civic interaction. At the same time, they come with numerous risks. In Africa's fledgling democracies, smart city technologies that are not related to security seem to have made life better for citizens. On the other hand, security-related smart city technologies have served to increase the power that political elites enjoy, at the expense of more robust democratic engagement. Given the pace at which technological development moves all across the world, this is an issue worth more sustained attention. As we have seen in the collapse of the Waterfront Toronto smart city project (Austen & Wakabayashi, 2020), informed and engaged activism is crucial to ensure that such technologies are acquired in ways that involve the people and used in ways that preserve their freedoms.

REFERENCES

Ahmad, N. (2009, July) Security Issues in Wireless Systems. [Master's Thesis], Blekinge Institute of Technology, 19. https://www.diva-portal.org/smash/get/diva2:833609/FULLTEXT01.pdf

Anderson, E. (2018). Freedom and Equality. *The Oxford Handbook of Freedom*, 4.

Austen, I. & Wakabayashi D. (2020, May 7). Google Sibling Abandons Ambitious City of the Future in Toronto. *New York Times.* https://www.nytimes.com/2020/05/07/world/americas/google-toronto-sidewalk-labs-abandoned.html

Azrour, M., Mabrouki, J., Guezzaz, A., & Kanwal, A. (2021). Internet of Things Security: Challenges and Key Issues. *Security and Communications Network 2021*(Article ID 5533843), 3. https://www.hindawi.com/journals/scn/2021/5533843/

Baraka, C. (2021, June 1). *The failed promise of Kenya's smart city.* Rest of Word. https://restofworld.org/2021/the-failed-promise-of-kenyas-smart-city/

Berry, I. (2021, November 19). 10 Ways AI can be used in smart cities. *AI Magazine.* https://aimagazine.com/top10/10-ways-ai-can-be-used-smart-cities

Chimhangwa, K. (2020, January 30). *How Zimbabwe's biometric ID scheme (and China's AI aspirations) threw a wrench into the 2018 election.* Global Voices Advox. https://advox.globalvoices.org/2020/01/30/how-zimbabwes-biometric-id-scheme-and-chinas-ai-aspirations-threw-a-wrench-into-the-2018-election/

China helps advance technology in Africa. (2022, January 12). *Global Times.* https://www.globaltimes.cn/page/202201/1245775.shtml

CISA. (2020, May 8). Securing Wireless Network. https://www.cisa.gov/uscert/ncas/tips/ST05-003

Cisco. (2017). Eight Things You Didn't Know About Cisco Systems. https://www.cisco.com/c/en_dz/about/blog-africa/2017/8-things-you-didnt-know-about-Cisco.html#:~:text=Cisco%20was%20officially%20incorporated%20on,%3A%20CSCO%20(Common%20Stock)

Cloud computing in Africa: Situation and Perspectives. (2012, April). *Telecommunication Development Sector*, 15-17. https://www.itu.int/ITU-D/treg/publications/Cloud_Computing_Afrique-e.pdf

Cooperation between Wilaya Von Dakhla and Huawei for the introduction of "Dakhla Smart City." (2021, May 31) *News Breezer.* https://newsbeezer.com/morroco/cooperation-between-wilaya-von-dakhla-and-huawei-for-the-introduction-of-dakhla-smart-city/

Crime Statistics. (n.d.) National Police Service. https://www.nationalpolice.go.ke/crime-statistics.html

Deutsche Welle. (n.d.-a). Africa embraces Huawei technology despite security concerns. https://www.dw.com/en/africa-embraces-huawei-technology-despite-security-concerns/a-60665700

Deutsche Welle. (n.d.-b) Investing in Africa's tech infrastructure. Has China won already? https://www.dw.com/en/investing-in-africas-tech-infrastructure-has-china-won-already/a-48540426

Duncan, J. (2018, June 4). *How CCTV surveillance poses a threat to privacy in South Africa.* The Conversation. https://theconversation.com/

how-cctv-surveillance-poses-a-threat-to-privacy-in-south-africa-97418

Elsewedy Electric. (n.d.) *About Us.* https://www.elsewedyelectric.com/en/about-us/

El Sewedy. Two French and Chinese companies win tender to supply smart meters for new capital. (2020, 28 January). *Enterprise.* https://enterprise.press/stories/2020/01/28/el-sewedy-two-french-and-chinese-companies-win-tender-to-supply-smart-meters-for-new-capital-10653/

Ethio Telecom to Pilot 5G Network in Ethiopia. (2021, December 7). *2merkato*. https://www.2merkato.com/news/alerts/6344-ethio-telecom-to-pilot-5g-network-in-ethiopia.

Etisalat Group. (n.d.). *About Etisalat*. https://www.etisalat.ae/en/etisalat-corporation.jsp

Feiner, L. (2019, August 14). Huawei employees intercepted encrypted messages to help African governments spy on political opponents, says WSJ. *Consumer News Business Channel*. https://www.cnbc.com/2019/08/14/huawei-employees-helped-african-governments-spy-on-opponents-wsj.html

Feldstein, S. (2019, September 17). *The Global Expansion of AI Surveillance.* Carnegie Endowment for International Peace.

Froehlich, A. (2021, December). WLAN security: Best practices for wireless network security. Tech Target. https://www.techtarget.com/searchsecurity/WLAN-security-Best-practices-for-wireless-network-security

Gallagher, R. (2019). Export Laws: China is selling surveillance technology to the rest of the world. *The Intercept* 48(3). https://journals.sagepub.com/doi/pdf/10.1177/0306422019876445.

Gravett, W. (2020). Digital neo-colonialism: The Chinese model of internet sovereignty in Africa. *African Human Rights Law Journal 2020*(20). http://www.scielo.org.za/pdf/ahrlj/v20n1/06.pdf

Green, W., Nelson, L., & Washington, B. (2020, May 1) *China's engagement with Africa: Foundations for an Alternative Governance Regime*. U.S-China Economic and Security Review Commission. https://www.uscc.gov/sites/default/files/2020-05/Chinas_Engagement_Africa.pdf

Hamama, B. (2020, 29 December). Morocco's Chinese Funded Tech City: the Shanghai of North-Africa? *Il Giornale dell' Architettura*. https://ilgiornaledellarchitettura.com/2020/12/29/moroccos-chinese-funded-tech-city-the-shanghai-of-north-africa/

Hawkins, A. (2018, 24 July). Beijing's Big Brother Tech needs African Faces. *Foreign Policy*.

Hayek, F. (1960). *The Constitution of Liberty.* University of Chicago Press.

Honeywell. (n.d.). About: Honeywell. *DBpedia*. https://dbpedia.org/page/Honeywell

Honeywell, Etisalat Misr. ACUD to deploy tech at Egypt's smart city. (2020, 19 January). *Construction Week*. https://www.constructionweekonline.com/products-services/262108-honeywell-etisalat-misr-acud-to-deploy-tech-at-egypts-smart-city

Huawei. (n.d.) Huawei helps the City of Ekurhuleni grow into a South African smart city pioneer. https://e.huawei.com/za/case-studies/za/south-african-smart-city-pioneer

Idris, A. (2021, August 9). The race to build Africa's 5G networks is entangled in a U.S. push to cut Huawei's dominance. *Rest of World.* https://restofworld.org/2021/the-race-to-build-africas-5g-networks-is-entangled-in-a-u-s-push-to-cut-huaweis-dominance/#:~:text=In%202020%2C%20when%20Safaricom%2C%20East,and%20its%20Finnish%20rival%2C%20Nokia.

Jili, B. (2020a, December 11). The Spread of Surveillance Technology in Africa Stirs Security Concerns. Africa Center for Strategic Studies. https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/

Jili, B. (2020b, December 29). Surveillance Technology a concern for many in Africa. *New Africa Daily.* https://newafricadaily.com/surveillance-technology-concern-many-africa

Kimuyu, H. (2021, November 17). Kenya: Public Outcry Forces Kura to Redesign Phase III of Killer Ngong Road. *AllAfrica.* https://allafrica.com/stories/202111180054.html

Large-scale infrastructure projects in Tangiers transforming and diversifying Morocco (n.d.) Oxford Business Group. https://oxfordbusinessgroup.com/analysis/smarter-city-large-scale-infrastructure-projects-are-transforming-urban-landscape

Minsait. (2019). *Minsait to implement a smart city in Casablanca which will serve as a model for the urban modernization of Morocco* [Press Release]. https://www.indracompany.com/sites/default/files/191011_pr_smartcitiescasablanca.pdf

Monika, G. (2016, November) Data Security is the Major Issue in Cloud Computing – A Review. *Indian Journal of Science and Technology 9*(43). https://www.researchgate.net/publication/311086550_Data_Security_is_the_Major_Issue_in_Cloud_Computing_-_A_Review

Moss, S. (2019, April 30). *Huawei to build Konza data center and smart city in Kenya, with Chinese concessional loan.* Data Center Dynamics. https://www.datacenterdynamics.com/en/news/huawei-build-konza-data-center-and-smart-city-kenya-chinese-concessional-loan/

Nokia. (2017). *Rwanda Government Pioneers Smart City Innovation with SRG and Nokia.* [Press Release]. https://www.nokia.com/about-us/news/releases/2017/05/16/rwanda-government-pioneers-smart-city-innovation-with-srg-and-nokia/

O'Grady, V. (2022, January 5). *Ghana's Celltel gets the go-ahead for major Wi-Fi project.* Developing Telecoms. https://developingtelecoms.com/telecom-technology/wireless-networks/12627-ghana-s-celltel-gets-the-go-ahead-for-major-wi-fi-project.html

Oirere, S. (2019). Ethiopia Goes for Automated Parking to Decongest City. *Parking Today Media*. https://www.parkingtoday.com/articledetails.php?id=2677&t=ethiopia-goes-for-automated-parking-to-decongest-city#:~:text=The%2015%2Dstorey%20Megenagna%20smart,a%20manufacturer%20of%20parking%20systems

Olander, E. (2022, January 4). *Ghana approves Homegrown Smart Cities Solutions that will use both Chinese and U.S. Tech*. China Global South Project. https://chinaafricaproject.com/2022/01/04/ghana-approves-homegrown-smart-cities-solution-that-will-use-both-chinese-and-u-s-tech/

Parvez, H. (2016). Smart Cities: A Global Perspective. *India Quarterly 72*(2).

Privacy International. (2021, November 18). *Huawei and Surveillance in Zimbabwe*. https://privacyinternational.org/long-read/4692/huawei-and-surveillance-zimbabwe#:~:text=Huawei%20has%20managed%20to%20secure,second%20largest%20Mobile%20Network%20Operator

Rahhou, J. (2021, November 9). Dakhla Smart City: A New Vision for Developing Southern Regions. *Morocco World News*. https://www.moroccoworldnews.com/2021/11/345431/dakhla-smart-city-a-new-vision-for-developing-southern-regions

Rahman, K. S. & Gilman, H. R. (2019). *Civic Power: Rebuilding American Democracy in an Era of Crisis.* Cambridge University Press.

Schwab, K. (2017, December 7). AI is reshaping what we know about cities. *Fast Company*.

Securing your wireless network. (n.d.). *Nibusinessinfo*. https://www.nibusinessinfo.co.uk/content/security-issues-wireless-networks

Shareholder Structure. (n.d.). Indra. https://www.indracompany.com/en/accionistas/shareholders-structure

Share price and profitability of the share Indra Sistemas A (MINSAIT). (n.d.) All Brands Markets. https://www.allbrands.markets/brand/price-share-stock-market-minsait-21460637100-es0118594417/

Sovereign Wealth Fund Institute. (n.d.). China Hi-Tech Group Corporation: State owned enterprise in China, Asia. https://www.swfinstitute.org/profile/598cdaa50124e9fd2d05ac82

Sun, Y., Zhang, J., Xiong, Y., & G. Zhu. (2014). Data Security and Privacy in Cloud Computing. *International Journal of Distributed Sensor Networks 2014*(Article ID 190903). https://journals.sagepub.com/doi/pdf/10.1155/2014/190903

Swejis, T., Maas, M., & Spiegeleire, S.D. (2017). Artificial Intelligence and the Future of Defense: Strategic Implications for Small and Medium sized Force Providers. *Hague Centre for Strategic Studies.*

The Wilaya of Dakhla and Huawei, a cooperation for the launch of Dakhla Smart City. (2021, June 1). Map News. https://www.mapnews.ma/fr/actualites/economie/la-wilaya-de-dakhla-et-huawei-une-coop%C3%A9ration-pour-le-lancement-de-dakhla-smart

Tomás, J. P. (2019, February 28). *Huawei delivering 5G networks in South Africa and Switzerland*. RCR Wireless. https://www.rcrwireless.com/20190228/5g/rain-huawei-announce-launch-first-5g-network-south-africa

TWI Global. (n.d.). *What is a Smart City?* https://www.twi-global.com/technical-knowledge/faqs/what-is-a-smart-city

What is Geospatial Technology. (2018). Bronx Community College. http://www.bcc.cuny.edu/academics/geospatial-center-of-the-cuny-crest-institute/what-is-geospatial-technology/

Why the government is moving towards smart cities. (2022, February 9). Enterprise. https://enterprise.press/hardhats/govt-moving-towards-smart-cities/

Wilkins, S. (2011, November 2). *Be Aware of These 7 Common Wireless Network Threats.* Plurasight. https://www.pluralsight.com/blog/it-ops/wireless-lan-security-threats

Woodhams, S. (2020, March 20). Huawei says its surveillance tech will keep African cities safe but activists worry it'll be misused. *Quartz Africa*. https://qz.com/africa/1822312/huaweis-surveillance-tech-in-africa-worries-activists/

APPENDIX

TABLE 1. Summary of the Acquisition and Use of Smart City Technology in Africa

Company	Public/Private	Availability of Contract for the Public	Public Participation in the Process Itself	Who Brokered the Deal	Foreign Gov't. Influence	Country
KENYA						
Huawei	Debated ownership; very plausible claim that it is controlled by the Chinese government.	N/A	Likely not	Unknown	Chinese gov't. is likely to assert influence on the co.; Article 7 of National Intelligence Law of the People's Republic of China.	China (Huawei, n.d.)
ETHIOPIA						
Dayang Auto-Parking Equipment Co. Ltd	Private company ("Dayang Auto-Parking Co Ltd," n.d.)	N/A	Likely not	Unknown	Chinese gov't. is likely to assert influence on the co.; Article 7 of National Intelligence Law of the People's Republic of China	China ("Dayang Auto-Parking Equipment Co Ltd," n.d.)
SOUTH AFRICA						
Huawei	Debated ownership; very plausible claim that it is controlled by the Chinese government.	N/A	Likely not	Unknown	Chinese gov't. is likely to assert influence on the com.; Article 7 of National	China (Huawei, n.d.)

Company	Public/Private	Availability of Contract for the Public	Public Participation in the Process Itself	Who Brokered the Deal	Foreign Gov't. Influence	Country
SOUTH AFRICA						
					Intelligence Law of the People's Republic of China	
GHANA						
Huawei	Debated ownership; very plausible claim that it is controlled by the Chinese government.	N/A	Likely not	Unknown	Chinese gov't. is likely to assert influence on the co.; Article 7 of National Intelligence Law of the People's Republic of China	China (Huawei, n.d.)
Celltel Networks Limited[1]	State-owned ("Celltel Networks," n.d.)	N/A	Likely not	Unknown	Likely not, as owned by Ghana	Ghana ("Celltel Networks Limited," n.d.)
EGYPT						
Honeywell	Publicly traded American multinational conglomerate corporation.	N/A	Likely not	Unknown	Unknown	USA ("Honeywell International Inc," 2010)
Etisalat Misr	Subsidiary of Etisalat Group. Only 40% of the company is traded publicly; the rest of the shares are owned by UAE government (Etisalat Group, n.d.)	N/A	Likely not	Likely UAE gov't. influenced co., as it owns the majority of shares (60%)	Most probably, the UAE government gets a 60% share in the company, with the remaining 40% traded publicly	UAE (Etisalat Group, n.d.)

1 Celltel Networks is a wholly-owned Ghanaian Internet Service Provider (ISP) offering nationwide affordable high-speed Wi-Fi network and 4G LTE mobile wireless services. Celltel's vision is to create smart cities, connecting at least one million homes and institutions nationwide in supporting government efforts to transform Ghana into a Digital Economy.

Company	Public/Private	Availability of Contract for the Public	Public Participation in the Process Itself	Who Brokered the Deal	Foreign Gov't. Influence	Country
EGYPT						
Elsewedy Electric	An Egyptian multinational electrical company founded by the Elsewedy family, listed on the Cairo stock exchange since 2006 (Elsewedy Electric, n.d.)	N/A	Likely not	Unknown	Likely not, as was founded by an Egyptian family before listed on stock-exchange	Company," 2022)
2 unnamed Chinese and French Cos.	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown
MOROCCO						
Minsait (parent organiza-tion is Indra Sistemas) (Minsait, 2019)	Publicly traded and listed on Madrid stock exchange ("Share price and profitability of the share Indra Sistemas," n.d.).[2]	N/A	Likely not	Unknown	Unknown	Spain ("Legal Information," n.d.)

2 The Company keeps no record of its shareholders, and thus is only aware of the composition of its shareholder structure through information provided to it by the shareholders themselves, whether directly or by public disclosure in accordance with the law governing significant ownership interests (which in general requires the reporting of stakes in excess of 3% of capital stock), and from data provided by Iberclear (Spanish Securities Clearing and Settlement Service), which Indra compiles for its Shareholders Meetings.

TABLE 1 REFERENCES

Celltel Networks Limited (n.d.). Dun and Bradstreet. https://www.dnb.com/business-directory/company-profiles.celltel_networks_limited.eebe29d190e628cea7433ba8443bc306.html.

Celltel Networks (n.d.). LinkedIn. https://gh.linkedin.com/company/celltel-networks.

China Communications Construction Company Limited. (2021, June 1). Fitch Ratings. https://www.fitchratings.com/research/corporate-finance/china-communications-construction-company-limited-01-06-2021

Dayang Auto-Parking Equipment Co Ltd, (n.d.) Export Hub. https://www.exporthub.com/dayang-auto-parking-equipment-co-ltd/

Dayang Parking Co Ltd. (n.d.) LinkedIn. https://www.linkedin.com/company/dayang-parking-co-ltd/

El Sewedy Electric Company S.A.E (Egypt). (2022, February 6) *In, On and For Emerging Markets*. https://www.emis.com/php/company-profile/EG/El_Sewedy_Electric_Company_SAE__%D8%A7%D9%84%D8%B3%D9%88%D9%8A%D8%AF%D9%89_%D8%A7%D9%84%D9%8A%D9%83%D8%AA%D8%B1%D9%8A%D9%83__en_2031563.html

Elsewedy Electric. (n.d.) *About Us*. https://www.elsewedyelectric.com/en/about-us/

Etisalat Group. (n.d.). *About Etisalat.* https://www.etisalat.ae/en/etisalat-corporation.jsp

Honeywell International Inc. (2010, February 23). United States Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/773840/000093041310000924/c60409_s-3.htm#:~:text=Honeywell%20was%20incorporated%20in%20Delaware,New%20Jersey%2C%2007962%2D2497

Legal information. (n.d.). Indra. https://www.indracompany.com/en/legal-information#:~:text=INDRA%20SISTEMAS%2C%20S.A.%2C%20holder%20of,M%2D11339%2C%20Page%2028

Minsait. (2019). *Minsait to implement a smart city in Casablanca which will serve as a model for the urban modernization of Morocco* [Press Release]. https://www.indracompany.com/sites/default/files/191011_pr_smartcitiescasablanca.pdf

Share price and profitability of the share Indra Sistemas. (n.d.). All Brands Markets. https://www.allbrands.markets/brand/price-share-stock-market-minsait-21460637100-es0118594417/

Shareholders structure. (n.d.). Indra. https://www.indracompany.com/en/accionistas/shareholders-structure.

Sichuan Haite High-Tech Co Ltd (China). (2021, December 12). *In, On and For Emerging Markets*. https://www.emis.com/php/company-profile/CN/Sichuan_Haite_High-Tech_Co_Ltd__%E5%9B%9B%E5%B7%9D%E6%B5%B7%E7%89%B9%E9%AB%98%E6%96%B0%E6%8A%80%E6%9C%AF%E8%82%A1%E4%BB%BD%E6%9C%89%E9%99%90%E5%85%AC%E5%8F%B8__en_1732580.html

Sichuan Haite High-Tech Company. (n.d.) Pitchbook. https://pitchbook.com/profiles/company/107821-36#overview

Tangier tech city plans revived with selection of Chinese giant CCC. (2019, May 1). *Global Construction Review*. https://www.globalconstructionreview.com/tangier-tech-city-plans-revived-selection-chinese/

Who are we. (n.d.). Huawei. https://www.huawei.com/minisite/whoishuawei/journey.html

A Tool or a Threat? The Adoption of Cryptocurrencies in Argentina

Maia Levy Daniel and Matías Jackson[1]

ABSTRACT:

This paper aims to identify the particular economic, financial, and social conditions that make Argentina one of the countries with the highest level of adoption of cryptocurrencies among its population and how this context should inform the government approach to crypto. For this, the paper reviews the scholarship studying the relationship between cryptocurrencies and human rights. Although the focus on the exercise of rights was present within earlier crypto communities, few studies approach this intersection, leaving room for new research. Additionally, the paper summarizes the economic context of Argentina over the last two decades and describes how the population is adopting cryptocurrencies to protect their earnings from inflation, as well as to purchase goods and services in their daily lives. The research concludes that, despite the wide adoption and declared benefits that crypto brings to citizens in Argentina, the government has approached regulation with contradicting signals and, in most cases, as a threat associated with illegal activities. In a context of wide adoption and financial instability, the potential impact of regulations on the exercise of human rights—particularly, the right to private property—is highly relevant and, therefore, policymakers should consider the international human rights framework.

KEYWORDS: Cryptocurrencies, bitcoin, human rights, freedom to transact, right to property, Argentina

1 INTRODUCTION

As in other regions, Latin America is witnessing a surge in the adoption of cryptocurrencies ("crypto"). The possibility of relying on a decentralized currency without government intervention seems like a golden promise in a region where political turmoil and economic unsteadiness have been the norm for decades. At the same time, countries in the region have turned to cryptocurrencies in different ways and for different reasons. For instance, El Salvador has recently become the first country in the world to pass a law adopting Bitcoin as a legal tender which, according to some analysts, may pave the way for the adoption in neighboring countries (Alvarez et al., 2022, Valkyrie Invest, 2021).

Argentina presents particular characteristics that have

1 The authors would like to thank Franco Amati, Olivia Goldschmidt, and Sandra Garin for their valuable insights on cryptocurrencies.

laid the groundwork for special interest in this new technology. As previously seen in Venezuela (Sharma, 2019), exceptionally high inflation rates, economic uncertainty, and a lack of trust in the country's institutions have been driving many Argentinians to buy crypto to store value and escape from political speculation through fiat money. Historical government measures with the aim of limiting citizens' capacity to decide what to do with their money and how to invest it laid the groundwork for people to look for alternatives. In this particular context, crypto is becoming a way to exercise basic needs, such as financial independence and the right to property.

Despite the increasing interest in the technology, studies on the region have focused on the regulatory and financial perspectives, as well as on government control. In addition, the use of crypto has often been related to financial speculation and money laundering. However, in countries with fragile institutions and strong economic interventions, regulations—depending on their approach and objectives—may interfere with human rights, such as the right to property. Although some stakeholders focus on the challenges this technology poses for states—the lack of government control and potential risks derived—cryptocurrencies are crucial for some groups in specific contexts in order to preserve their financial resources, limiting the power from governments and, ultimately, protecting these groups' own freedom.

In fact, the use of cryptocurrencies can be key in limiting the power of governments to punish citizens for questioning their policies. For example, although Canada has always been categorized as a strong democracy with access to political rights and civil liberties (Freedom House, 2022), recent anti-government protests led to decisions to freeze protesters' bank accounts, which portrays an example of the potential dangers involved (Fung, 2022).

Taking Argentina as a case study in the region, we aim to identify the particular economic, financial, and social conditions that lead to the adoption of cryptocurrencies and regulations, and the potential impact of regulations on the exercise of human rights. In this article we address the whole universe of cryptocurrencies—a form of digital assets based on a network distributed across a large number of computers—without analyzing the technology itself (Frankenfield, 2022). First, we offer a brief overview of the main studies on cryptocurrencies and their relationship with human rights, as well as the arguments developed both by supporters of crypto and opposing groups. Second, we briefly describe the Argentine economic context, highlighting the main facts and events of the last two decades that will set the scene for the analysis. Third, we characterize the use of cryptocurrencies in Argentina, detailing the specific features that make people decide to turn to these currencies, their strengths and disadvantages, how the government has responded to this phenomenon, and the potential impacts on human rights. In addition, we address the difficulties and threats regulations may entail in this context, the economic and social impacts, and how the analysis and conclusions may also apply to countries in similar situations of economic distrust and high volatility. Finally, we provide main findings and recommendations on dimensions that governments can incorporate in their policy decisions.

2 CRYPTOCURRENCIES AND HUMAN RIGHTS

The relationship between crypto and human rights dates back from the very first idea of a cashless society envisioned by cypherpunks. This digital activist group advocated for the defense of freedom to conduct anonymous economic transactions by using cryptography. In 1993, Eric Hughes, author of the Cypherpunk Manifesto, claimed that "privacy in an open society requires anonymous transaction systems," so they made a call to "create systems which allow anonymous transactions to take place" (Hughes, 1993). On the political spectrum, cypherpunks were mostly aligned with libertarian ideology (Jarvis, 2021).

A couple of decades later, these cypherpunks' ideas were present in Satoshi Nakamoto's seminal paper in which Bitcoin was introduced.[2] He proposed a new model

2 "Bitcoin is a non-fiat cryptographic electronic payment system that purports to be the world's first cryptocurrency. In other words, it is a peer-

of privacy protection through anonymous public keys (Nakamoto, 2008). Although the effective level of privacy of Bitcoin has been challenged due to the public record of transactions, there is agreement that pseudonymity provides higher standards for privacy protection, especially when compared with traditional centralized systems (Van Valkenburgh, 2015).

More recently, the crypto community has supported the adoption of cryptocurrencies as part of a so-called "freedom to transact" (Silverman, 2022). Especially after the blockade of Bitcoin addresses in Canada and the Russian invasion of Ukraine, which has triggered numerous financial sanctions on Russian citizens, the cryptocurrency promoters have returned to the roots of the crypto-libertarian ideology. Supporters argue this right is a combination of the freedom of speech and the right to privacy, which stem from the first and fourth amendments of the U.S. Constitution (Van Valkenburgh, 2019).

Despite the growing interest in this "freedom to transact" mantra, Renieris (2022) points out that this right is not enshrined in any of the international human rights instruments. The absence of this concept in the legal framework prevents an analysis through the lens of interdependence and potential tensions with other human rights. This derives from a frequent absolutism from the crypto community that may undermine other individual rights and freedoms: "The every-man-for-himself ethos of crypto-libertarians who seek to disrupt, disintermediate and destabilize institutions directly undermines our ability to respond to such crises as a society, thereby endangering all other individual rights and freedoms" (Renieris, 2022).

Although the "freedom to transact" as defended by crypto pioneers is not part of the international human rights framework, the "right to property" can function as a proxy. In this sense, the international and regional human rights instruments and court decisions could provide valuable insights and principles to analyze the use of cryptocurrencies from a human rights perspective. The Inter-American System of Human Rights (IASHR) established that "Every person has the right to use and enjoy their property. The law may subordinate such use and enjoyment to social interest" (Article 21 of the American Convention on Human Rights). On the basis of this Article, the Inter-American Court of Human Rights developed a broad interpretation of the protection of property, defined as "appropriable material things, as well as any right that may form part of a person's assets" (Case Barbani Duarte and Other v. Uruguay, 2011, p. 237).

Although the "freedom to transact" as defended by crypto pioneers is not part of the international human rights framework, the "right to property" can function as a proxy.

Picking up the human rights position from a different perspective, Rueckert (2019) analyzes cryptocurrencies' regulations through the lens of the European Union's human rights framework. The author highlights the little attention that has been given to the impact cryptocurrencies regulations may have on human rights: "Most governments seem to focus exclusively on possible damage and criminal activities as well as possibilities of taxation in connection with cryptocurrencies, without considering the human rights of the individuals and legal entities involved" (Rueckert, 2019, p. 9). To start filling this gap, he analyzes the human rights that may be impacted through anti-money-laundering (AML) and crime-prevention regulations, either traditional regulations or new ones specifically created for cryptocurrencies. Among the impacted rights, the author identifies the following:

- *Personal data and private life:* Transaction data in the blockchain can be considered personal data, within the scope of the European data protection framework. Therefore, government agencies may violate these rights through preventive or research measures, such as the systematic collection, storage, and/or processing of data from the blockchain, or by mandating companies to retain certain information for a period of time.

- *Right to property:* Due to certain cryptocurrencies' characteristics (rivalrousness, persistence, interconnectivity, definability, and market value), they meet the criteria for being considered "virtual currency" and therefore are protected by the right to property. Some of the interferences to this right could be measures of expropriation, confiscation, or seizure.

- *Right to pursue a trade or profession:* In the cryptocurrency ecosystem, this right is meant to protect anyone who conducts a profit-oriented business, such as professional traders, investors, operators of exchange platforms, and data miners. Regulations that implement Know Your Customer systems or due diligence must comply with this right.

- *Freedom of association:* Considered as a network established and run on a voluntary basis for a stable period, the main cryptocurrency, Bitcoin, can be deemed an association under the terms of the European Human Rights framework. Therefore, regulations that restrict the crypto community or access to their networks, such as a complete ban, interfere with the right to freedom of association.

- *Freedom of expression and freedom of information:* The wide interpretation on the right to freedom of expression in the European Human Rights framework protects "any form of communication" with "any content," which includes cryptocurrency transactions. Therefore, this right protects (1) the sending, (2) the receiving, and (3) the access to any publicly available information.

As long as governments' concerns and attention have focused on investigating and prosecuting the use of cryptocurrencies for criminal activities, legal scholarship seems to have followed the same path. The literature review shows a tendency to approach cryptocurrency regulations from the perspective of abuses and illegal activities rather than the possibilities they may bring to users. In this sense, Rueckert (2019) noted that "no examination of the relation between AML regulation, crime prevention, criminal investigation and fundamental rights in the particular context of cryptocurrencies has been published," and concluded that "future legal research should enhance the relationship between cryptocurrencies, governmental means and fundamental rights." Although it is outside the scope of this article and further analysis would be needed to reach such a conclusion, based on the research done for this article, it is plausible to affirm that this relationship Rueckert mentions has been largely overlooked by legal scholarship.

Fletcher et al. (2021) point out that, despite the benefits Bitcoin may entail for unstable societies, its widespread adoption has become a matter of concern for government agencies. Fueled by the abuse of Bitcoin as a means for terrorism and crime, countries have started a "bureaucratic turf war over regulation."[3] By reviewing the regulatory responses from U.S. financial agencies, the authors conclude that none of the perspectives or frameworks proposed "truly account for the unique properties of Bitcoin as well as users' interests in a secure system of transactions

to-peer, client-based, completely distributed currency that does not depend on centralised issuing bodies (a 'sovereign') to operate. The value is created by users, and the operation is distributed using an open source client that can be installed on any computer or mobile device" (Guadamuz & Marsden, 2015).

3 For instance, in 2018, the undersecretary for terrorism and financial intelligence for the U.S. Department of the Treasury, Sigal Mandelker, highlighted that terrorists and other criminals have used cryptocurrency to "exploit the financial system," "hide their ill-gotten gains," and "finance their illicit activities," and called for regulators to "make haste in cracking down on regulations for the safety of cryptocurrency and its investors" (Butera, 2018).

that is safe from the purview of government entities." They warn that these competing narratives and the threat of overregulation "may push users to seek illicit means to use Bitcoin and avoid regulation altogether."

In this sense, governments from around the world have focused their attention on crime prevention and/or taxation. For example, Nica et al. (2017) reviewed how cryptocurrencies have been used in multiple kinds of illegal activities, such as in money laundering, tax evasion, terrorism financing, and dark markets development.

Another challenge governments address as cryptocurrencies move from niche to broad adoption is how to classify them for taxation purposes. The question of whether they constitute assets, currency, a payment system, or something else is a major challenge for national administrations as well as international organizations (Katarzyna, 2019).

These trends of preventing illegal activities and promoting taxation have led national authorities to explore different types of regulations and approaches (Blemus, 2017; Global Legal Research Center Staff, 2018). While some countries completely banned their use (like Bolivia and Russia), others issued amendments or clarifications to existing regulations on taxation or anti-money-laundering, and others have not yet adopted a formal position (International Monetary Fund, 2016).

3 THE ARGENTINE ECONOMIC CONTEXT

The economic context in Argentina is peculiar even within the region. The socioeconomic scenario has been impacted by frequent financial and economic crises, overly high inflation rates, lack of trust in banks, and strong disappointment in the government and representatives in general. Particularly, there have been some developments and facts that seriously affected the legitimacy of the country's latest administrations and institutions. A comprehensive description and analysis of Argentina's economic history would definitely require a whole paper; however, a few facts are worth mentioning to understand the context.

Inflation rates have seriously affected the Argentine economy throughout the country's history. While rates have varied over the years, average two-digit rates prevailed between 1945 and 1975. Between 1975 and 1988, Argentina experienced a period of three-digit inflation rates—with peaks of 444% in 1976, 626.7% in 1984, and 672.2% in 1985 (Gerchunoff & Llach, 1998, pp. 469-471). In 1989 and 1990, Argentina faced hyperinflation, with peaks of 3,079% and 2,314%, respectively (Gerchunoff & Llach, 1998, pp. 469-471). This phase ended with the "Convertibility Plan," which pegged the Argentine peso to the U.S. dollar. However, in 2001 inflation rose again, with average rates of 20-25% between 2002 and 2017, and peaks of 47.6% and 53.8% between 2018 and 2019 (Canitrot, 2018; Statista 2022).[4]

Between 1998 and 2002, Argentina faced one of the greatest economic, financial, political, and social crises in its history. On December 1, 2001, with the aim of preventing a financial collapse, the administration implemented a "Corralito" (freezing of financial assets) through a national decree (Government of Argentina, 2001). This measure limited the amount of cash people could withdraw from their bank accounts to avoid widespread panic and a collapse of the bank system. Although electronic transfers were permitted, at the time only 1% of the transfers were made by debit and credit cards, so this measure resulted in commercial stagnation (Smink, 2021). Withdrawals in dollars were not allowed. Furthermore, wire transfers abroad were prohibited.

Thousands of people poured into the streets across the country to complain and protest against the economic situation and the government's measures. In general, people were self-convened and did not respond to any political

4 It is worth mentioning that between 2007 and 2015, the Instituto Nacional de Estadísticas y Censos (INDEC), the agency in charge of measuring, among other things, the country's levels of inflation, unemployment, and poverty, was interfered with by the government. The administration at the time replaced INDEC's authorities with people aligned with their political views. As a result, and owing to their lack of accuracy, civil society organizations have pointed out that INDEC's statistics and figures during that period have been considered unreliable (Slipczuk, 2019).

party, union, or social organization. The socioeconomic crisis and discontent resulted in the resignation of President Fernando de la Rúa and his Minister of Economy, Domingo Cavallo, on December 21, 2001.

Between 1998 and 2002, Argentina faced one of the greatest economic, financial, political, and social crises in its history.

After De la Rúa's resignation, five presidents held office over five months, and institutional instability was undeniable. During the presidency of one of De la Rúa's successors, Eduardo Duhalde, U.S. denominated debt and deposits were exchanged for Argentine pesos—a measure named "Corralón" (law freezing bank term deposits), replacing the Corralito—and account holders had their savings converted into a less-valued currency. Over the years, representatives lost credibility and there was a general popular demand for "que se vayan todos" ("all of them must go"), aiming for all representatives and politicians to resign. The country experienced a general disbelief in institutions, in the ability of governments to face the crisis, and in representatives in general. This situation would extend over the following years.

Furthermore, Argentina implemented a "cepo cambiario" (foreign currency control) at different times in the last decade. This measure limits the purchase of foreign currency with the aim of preventing the local currency from depreciating. The measure was first applied in 2011, during the administration of President Cristina Fernández de Kirchner (Government of Argentina, 2011). Individuals and companies needed an authorization to purchase foreign currency granted by the Argentine tax agency—AFIP—and individuals were allowed to spend only up to 40% of their salaries. The cepo cambiario was strengthened over the years, restricting even more the amount of foreign currency destined to both savings and the purchase of products in even more sectors (Scarpinelli, 2015). Moreover, imports were prohibited (Scarpinelli, 2015). In 2015, the Macri administration lifted this measure, but had to reimplement it in 2019 before leaving office (Slipzuk, 2020). Currently, each person is allowed to purchase up to USD 200 per month—only if certain requirements are met—or less if part of that amount has already been used to buy products or services abroad—for instance, online purchases (Barbería, 2019; Infobae, 2021; El Cronista, 2021)

Although not every measure is currently in effect, the consequences of all these events remain. The role the government has played in the purchase and use of foreign currency and in the account holders' ability to access and manage their savings has caused Argentinians to distrust the country's institutions and representatives. Given the restrictions still in place and the futility of the measures taken by most recent governments to stop high inflation rates, the feeling of suspicion and distrust is still very strong. The lack of investment and savings capacity owing to the depreciation of the Argentine peso over the years has raised the existing levels of disappointment and the lack of hope. Moreover, this perception has increased nowadays due to the high levels of unemployment and informal employment at the national level (INDEC, 2021), the country's economic stagnation (IProfesional, 2022), and the rising tax rates and new taxes, without clear improvements of public services that justify them.

4 CRYPTOCURRENCIES IN THE ARGENTINE SCENARIO

As described in the previous sections, particular characteristics of the Argentine context make cryptocurrencies an attractive alternative to the local currency. First, high inflation rates lead Argentinians to look for ways to get rid of Argentine pesos. Earnings in pesos depreciate every day, so people are willing to exchange them as soon as possible for any other currency to preserve at least part of their value. In addition, unexpected economic changes and lack of legal certainty make Argentinians look

for alternatives to save their money. This scenario couples with the various foreign currency controls implemented over the last decade. People see how their earnings in Argentine pesos depreciate, but they have limitations on the amount of foreign currency they can buy. This leads to a lack of investment and savings capacity that cryptocurrencies are able to tackle. Moreover, fiat money requires strong institutional mechanisms of independence, accountability, and oversight (Chohan, 2021), three characteristics that are not common among Argentine institutions.

Therefore, for many Argentinians, the use of cryptocurrencies has become a way to protect their earnings not only from inflation but also from restrictions on the use of those earnings (Ro, 2022). The country ranks tenth in the Global Crypto Adoption Index among 154 countries, only surpassed by Venezuela in the region. According to the study, Latin America accounts for only 9% of all transaction activity, with a high predominance of peer-to-peer (P2P) trading. Although the study does not go deeper into the Argentine case, it points out that in this country there has been a correlation on the value of the peso and the crypto trade volume: "As the Argentine peso loses value steadily over the time period studied, P2P trade activity tends to increase" (Chainalysis, 2021, p. 41).

Because they are decentralized, cryptocurrencies cannot be manipulated or mismanaged by monetary authorities (Chohan, 2021). As expressed by experts in the field, the use of cryptocurrencies in Argentina is very different from the use in other countries. For instance, Argentina has a high proportion of employees who get their salaries in cryptocurrencies; their companies are allowed to pay up to 20% of their remuneration in this currency (Serrano-Román & Olivera Doll, 2022). Moreover, Argentina has become a perfect place for crypto mining, primarily due to the low cost of electricity fees. Since electricity is subsidized by the national government, Argentina is placed 12th out of 100 countries analyzed by the Global Petrol Prices ranking of electricity prices for businesses (Global Petrol Prices, 2021). While the world average price is 0.125 USD per kWh for businesses, Argentina's average price in 2021 was 0.036.[5]

For many Argentinians, the use of cryptocurrencies has become a way to protect their earnings not only from inflation but also from restrictions on the use of those earnings.

In April 2022, the local consultancy firm Taquion published a study on Argentinians' perceptions on crypto and its adoption. According to the research, three out of ten Argentinians know what cryptos are and how to use them. Of those who use or have used crypto, 34% have done it because it is not sensitive to inflation, while 64% of Argentinians think there is a favorable scenario for the adoption of cryptocurrencies in the country given the lack of confidence in local currency (Taquion, 2022).

A few regulatory developments not only by the national government but also by local governments are worth

5 In December 2021, neighborhoods across several cities experienced electricity shutdowns. The public-private company in charge of electricity distribution, CAMMESA, began an investigation to check the relationship of these cuts with the usage of crypto farming companies (Glezer, 2021). The impact of cryptocurrencies on the environment is a highly debated topic all over the world (for instance, see Badea & Mungiu-Pupazan, 2021, and Reiff, 2021). Although there might be a link between the use of cryptocurrencies, and human rights and the right to a sustainable environment, this falls outside the scope of this paper.

mentioning.[6] In March 2022, the Argentine government sent a letter of intent to the International Monetary Fund (IMF) for debt restructuring so it can avoid default (Ministry of Economy of the Republic of Argentina, 2022). According to the document signed by the national Minister of Economy, Argentina pledged to "discourage the use of crypto-currencies with a view to preventing money laundering, informality and disintermediation." The agreement shook the regulatory agenda of cryptocurrencies in the country. After the announcement, local press reported that the Unit of Finance Information is working to add cryptocurrency service providers to the list of entities subject to reporting and recording customer transactions (Olivera Doll, 2022).[7]

However, in April 2022, the Government of the City of Buenos Aires announced that in the following months it would enable the ability to pay taxes using cryptocurrencies (Engler, 2022). Authorities clarified that although taxpayers would be able to use this new payment channel, the government would not receive any crypto but the equivalent in Argentine pesos through local exchanges acting as intermediaries.

In May 2022, two national banks announced they would start offering their clients the option to buy cryptocurrencies through their home banking systems. Banco Galicia, one of the banks that announced the measure, declared they had performed a survey among their clients and concluded that more than 60% wanted to operate with cryptos (Della Vecchia, 2022). However, a couple of days later, the Argentine Central Bank issued an order prohibiting all banks from operating with cryptocurrencies because of the risks they may entail.

The 2022 Argentine winter was accompanied by a "cryptowinter": Currencies significantly devalued or directly crashed after four years of continued growth (Browne, 2022; Chohan, 2022). While Bitcoin price went from its all-time high of nearly USD 69,000 in November 2021 down to USD 19,000 in September 2022, some other currencies, paradoxically called Stablecoins, collapsed (Sier & Hewitt, 2022). The most noticeable case was TerraUSD, a stablecoin supposed to be attached to the USD value, fell down to USD 0.30 on May 11. Following these events, local and international media outlets reported stories on how this crash affected Argentinians who had moved their savings to different cryptocurrencies (Lankes, 2022). Some testimonies informed the loss of life savings: "They scammed [me]. I have nothing left, not even a penny" (Schwartz & Idris, 2022).

However, the Argentine economic and political scenarios seem to overshadow the crypto risks. In July 2022, on the day the Minister of Economy, Martín Guzman, stepped down, specialized websites reported an increase between two and three times in the purchase of stablecoins compared to a "typical Saturday" (Jamele, 2022).

This brief summary on the different advances and setbacks for crypto adoption in Argentina allows us to derive some findings.

5 MAIN FINDINGS AND CONCLUSIONS

The peculiar socioeconomic context of Argentina has paved the way for a set of particularities in the adoption of cryptocurrencies. A history of economic instability and distrust in the local currency, along with the recent restrictive measures and high inflation rates, have turned crypto into an escape valve different from what can be reported in other countries, especially developed ones. In a certain way, the current scenario seems to be the

6 In addition, a few financial and tax regulations at the national level are also relevant. In 2014, the Unit of Finance Information, a federal agency, approved Resolution 300/2014 warning financial institutions to pay special attention to crypto operations and to establish a reinforced control. Since 2018, the Federal Administration for Public Funds (AFIP) has taxed profits from the sale of crypto. In addition, in 2019, this same office mandated crypto exchanges to report their operations monthly. In November 2021, the Decree 796/2021 included the operations of sell and buy in the Tax Over Credits and Bank Debits (ICDB).

7 The ruling party "Frente de Todos" presented a bill to Congress on the creation of a National Fund for Canceling the Debt with the IMF. The bill, which has already passed the Senate Chamber, establishes a tax on goods located outside the country, including crypto assets, which have not been previously declared to the AFIP, with the objective of creating a fund for canceling the debt of more than 44 billion USD (Distéfano, 2022; Senado Argentina, 2022).

most representative example of the original cypherpunks' libertarian spirit to defy governmental institutions through a decentralized way to exchange goods and services.

This perspective allows us to draft some findings on how the people and the government perceive cryptocurrencies, and their approach to them.

First, the country is going through a broad adoption of cryptocurrencies as a mechanism to protect from inflation and fiat money volatility. As one of the experts consulted for this paper pointed out, "in Argentina regular people buy crypto, it is a grassroot movement." Despite their volatility and the difficulties of using crypto in their daily lives, some people prefer cryptos rather than Argentine pesos, as a way of both saving and paying for goods and services.

According to a survey conducted by Morning Consult in June 2022 (Morning Consult, 2022), seven out of the top ten countries adopting crypto—a list in which Argentina is included—have some form of foreign exchange or capital controls. When describing the Argentine scenario, the consultancy firm states: "local currency and government bonds see less confidence than cryptocurrency as a store of value. Coupled with ... Argentina's macro instability and high inflation, this indicates that cryptocurrencies may be viewed as a viable store of value when local assets aren't good alternatives, and especially when it is difficult to move capital outside the country" (Morning Consult, 2022, p. 23).

As reported by the media, the 2022 crash may have represented a challenge for those Argentinian crypto adopters. However, if and how it may impact the adoption in Argentina in the long term remains to be seen. In the meantime, the economic and institutional crisis has deepened: the government named three economic ministers in a month and inflation was expected to reach 100% by the end of 2022 (Gillespie & Squires, 2022; Gillespie, 2022).

Second, the governmental approach to crypto shows some contradictions in the promotion or discouragement of its use. By the time the Government of the City of Buenos Aires, the country's main city, announced the possibility to pay taxes with bitcoins, the national government was signing a pledge with the IMF to discourage crypto in order to prevent "money laundering, informality and disintermediation." These contradictory signals, which may be because opposing political parties sit in each administration, make it more complex to define how Argentina positions itself in this boom of cryptocurrency adoption.

However, based on the regulation reviewed, it can be affirmed that national government regulation has approached crypto as a threat. In this sense, national authorities around the globe have followed the trend toward a "bureaucratic turf war over regulation" (Fletcher et al., 2021), focusing on the alleged threats of crime and tax evasion. Despite the declared benefits that the technology seems to bring to a part of the Argentinian population, government agencies are following the thread as a matter of concern and so are trying to discourage its use. The Argentine government is not taking into account the specific context that needs to inform its policies nor considering the local implementation and consequences, which should be integral.

This approach might also represent an example of how the medium is sometimes confused with the end. People may use crypto for money laundering and illegal activities, but it is not the only or even the main purpose of cryptocurrencies. Cash and other currencies or assets may also be used for the same purpose. General bans or tough controls on cryptocurrencies and their users may cause harm more than they benefit the population. A deep understanding of the particular problem in the local context is necessary in order to design and implement evidence-based policies.

Third, and directly associated with the threats approach noted before, regulation of the use of crypto has not taken human rights into consideration. Considering the specific uses and widespread adoption of crypto in Argentina, this dimension might be of special relevance.

As reported in the Cryptocurrencies and Human Rights section, it is plausible to affirm that the relationship between cryptocurrencies, governmental means, and human rights has been largely overlooked by legal

scholarship. Taking into account the reasons why crypto is being adopted in Argentina and its specific conditions—as described in previous sections—the right to property and how it can be restricted by governments might be of particular interest. In this sense, as previously mentioned, the Inter-American System of Human Rights (IASHR), to which Argentina adheres, has established the protection of a broad concept of property. In addition, the Inter-American Court of Human Rights (IACHR) has indicated that "the restriction of the rights enshrined in the Convention must be proportional to the interest of justice and closely adjusted to the achievement of that objective, interfering as little as possible in the effective exercise of a right" (Case Salvador Chiriboga v. Ecuador, 2011). Thus—although the IACHR does not address cryptocurrencies explicitly—arguments by the Central Bank based on broad terms such as "potential vulnerabilities" or "potential failure to comply with current exchange regulation" to limit the purchase of crypto may not comply with the principles established by the IASHR (BCRA, 2022).

National government regulation has approached crypto as a threat. ... [it] has not taken human rights into consideration.

The Court has also said that, in order to be compatible with the American Convention of Human Rights, deprivations of a person's property must "be based on reasons of public utility or social interest, subject to the payment of fair compensation, practiced according to the cases and forms established by law" (Case Salvador Chiriboga v. Ecuador, 2011). In conclusion, if the government intends to impose restrictions on the purchase or use of cryptos, it should consider the principles established by the IASHR and its limitations.

Regarding this third finding, although a more thorough and practical analysis on this particular issue needs to be done in the future, the arguments intend to bring human rights to the discussion and provide an innovative approach that could be used to conduct further research on crypto regulations.

6 KEY POLICY RECOMMENDATIONS

Although the Argentine case might not be representative of developing countries in the Global South or even in the Latin American region, the country presents a case study for widespread adoption of crypto in a context of general distrust in fiat money, politicians, and economic institutions. According to the findings of this research, decision-makers facing this kind of scenario and willing to intervene should incorporate the following dimensions into their analysis:[8]

1. *Recognize that crypto can be a tool.*

First, a widespread-use scenario means more interests at stake and pressure on how to regulate private activities. In this sense, decisions on cryptocurrencies could benefit from a multistakeholder approach that contemplates not only the government's concerns but also the possibilities that the tool brings to the public.

8 A brief disclaimer should be made here in regard to political decisions on cryptocurrency regulations. The recommendations in this section are specifically based on the particular characteristics of the Argentine case. The purpose of the recommendations is limited to highlight issues that should be taken into account by decision-makers in a widespread scenario, with a low government credibility, as well as with foreign exchange controls, representing a context that the early crypto community has depicted and longed for since its very beginning. Whether countries—or Argentina—should regulate the use of crypto, approve crypto-friendly rules, or even completely ban them is a debated question and this article does not intend to address it. In this sense, our recommendations fit into a broader question: What should policymakers look at when willing to intervene? To answer this question, decision-makers should adopt a human rights framework that should permeate and guide every measure. As we summarized in the article, the intersection between crypto technologies, its regulation, and governmental control needs further analysis from a human rights perspective and this perspective should permeate every policy decision.

economic instability. In such a scenario, the country could benefit from the technology and its possibilities relating to financial inclusion and literacy, as well as changes in the productive and economic industry.

An interdisciplinary and context-based approach could inform better policy decisions that aim to benefit the population.

2. Understand that crypto is not necessarily a threat.

First, adopting regulation only to respond to illegal activities such as money laundering and tax evasion might be short-sighted and ignore other explanations for the widespread use and willingness to buy crypto, especially in the context of economic turmoil and instability.

For this reason, second, the possibilities that the technology enables for legal activities must be incorporated. This requires a change of perspective, from a threat to an enabler approach, which probably differs from what is mandated by international finance institutions.

Third, governments should check the signals they send to citizens on the promotion or discouragement of the adoption of these technologies. Coordination between the national and local governments is key to achieving coherent results and to offering legal and regulatory certainty.

3. Consider the human rights framework.

First, in contexts of high inflation rates and government controls, crypto may be considered a way to access basic goods and services. Governments should take into account that, in this context, some people may have their savings or salaries in cryptocurrencies and would need them to develop their lives.

Second, imposing limitations on the use of cryptos may be considered a limitation on the fundamental right to property. When adopting limits on the acquisition or ownership of these goods, authorities should take into consideration regional and international human rights instruments, such as the principles established by the IASHR.

REFERENCES

Alvarez, F., Argente, D., & Van Patten, D. (2022). Are Cryptocurrencies Currencies? Bitcoin as Legal Tender in El Salvador. University of Chicago, Becker Friedman Institute for Economics Working Paper No. 2022-54. Available at SSRN: https://doi.org/10.2139/ssrn.4094160

Alzahrani, S., & Daim, T. (2019). Analysis of the Cryptocurrency Adoption Decision: Literature Review. *2019 Proceedings of PICMET '19: Technology Management in the World of Intelligent Systems*.

Badea, L., & Mungiu-Pupazan, M. C. (2021). The Economic and Environmental Impact of Bitcoin. *IEEE Access*, *9*, 48091–48104. https://doi.org/10.1109/access.2021.3068636

Barbería, M. (2019, October 28). Endurecen el cepo: baja a U$S 200 el tope a las compras mensuales. *El Cronista.* https://www.cronista.com/finanzasmercados/Endurecen-el-cepo-baja-a-us-200-el-tope-a-las-compras-mensuales-20191028-0004.html

BCRA (Banco Central de la República Argentina). (2022). El BCRA desalienta la oferta de criptoactivos a través del sistema financiero. https://www.bcra.gob.ar/Noticias/BCRA-desalienta-oferta-criptoactivos-sistema-financiero.asp.

Blemus, S. (2017). Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide. *Revue Trimestrielle de Droit Financier (Corporate Finance and Capital Markets Law Review) RTDF, 4*. Available at SSRN: https://doi.org/10.2139/ssrn.3080639

Browne, A. K., Ryan. (2022, July 14). *This "crypto winter" is unlike any downturn in the history of digital currencies. Here's why.* CNBC. https://www.cnbc.com/2022/07/14/why-the-2022-crypto-winter-is-unlike-previous-bear-markets.html

Butera, C. (2018, February 15). *US Treasury Official Pushes for Worldwide Cryptocurrency Regulation Against "Kleptocrats and Criminals."* Chief Investment Officer. https://www.ai-cio.com/news/us-treasury-official-pushes-worldwide-cryptocurrency-regulation-kleptocrats-criminals/

Canitrot, A. (2018, July). Historia de la inflación en Argentina. https://www.cac.com.ar/data/documentos/10_Historia%20de%20la%20inflaci%C3%B3n%20en%20Argentina.pdf

Case Barbani Duarte and Other v. Uruguay. (2011). (Inter-American Court of Human Rights).

Case Salvador Chiriboga v. Ecuador. (2011). (Inter-American Court of Human Rights).

Chainalysis. (2021). *The 2021 Geography of Cryptocurrency Report*. chainalysis.com

Chohan, U, W. (2021). Cryptocurrencies and Hyperinflation. *Critical Blockchain Research Initiative (CBRI) Working Papers*. UNSW Business School. https://ssrn.com/abstract=3320702

Chohan, U. W. (2022, June 19). Crypto Winters. *Critical Blockchain Research Initiative (CBRI) Working Papers*. UNSW Business School. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4142885

Della Vecchia, N. (2022, May 3). Paso a paso, cómo comprar criptomonedas desde el home banking del Banco Galicia. *Forbes Argentina.* https://www.forbesargentina.com/innovacion/paso-paso-como-comprar-criptomonedas-home-banking-banco-galicia-n15559

Distéfano, B. (2022, March 31). *Impuestazo a bitcoin para pagar deuda argentina: el nuevo proyecto de ley*. CriptoNoticias - Noticias De Bitcoin, Ethereum Y Criptomonedas. https://www.criptonoticias.com/finanzas/impuestazo-bitcoin-pagar-deuda-argentina-proyecto-ley/

El Cronista. (2021, October 6). Súper cepo al dólar: una por una, todas las restricciones vigentes y qué alternativas quedan. https://www.cronista.com/finanzas-mercados/super-cepo-al-dolar-una-por-una-todas-las-restricciones-vigentes-y-que-alternativas-quedan/

Engler, A. (2022, April 26). La Ciudad de Buenos Aires habilitará el pago de impuestos con criptomonedas. *Coindesk*. https://www.coindesk.com/policy/2022/04/26/la-ciudad-de-buenos-aires-habilitara-el-pago-de-impuestos-con-criptomonedas/

Fletcher, E., Larkin, C., & Corbet, S. (2021). Countering money laundering and terrorist financing: A case for bitcoin regulation. *Research in International Business and Finance, 56*, 101387. https://doi.org/10.1016/j.ribaf.2021.101387

Frankenfield, J. (2022, January 11). Cryptocurrency. In *Investopedia*. https://www.investopedia.com/terms/c/cryptocurrency.asp

Freedom House. (2022). *Freedom in the World 2022 - Canada.* https://freedomhouse.org/country/canada/freedom-world/2022

Fung, K. (2022, February 18). Banks Have Begun Freezing Accounts Linked to Trucker Protest. *Newsweek*. https://www.newsweek.com/banks-have-begun-freezing-accounts-linked-trucker-protest-1680649

Gerchunoff, P. & Llach, L. (1998). *El ciclo de la ilusión y el desencanto.* Ariel Sociedad Económica.

Gillespie, P. (2022, September 7). *Argentina Inflation Rate to Hit 100% by End of 2022, EcoGo Says*. Bloomberg. https://www.bloomberg.com/news/articles/2022-09-07/argentina-inflation-rate-to-hit-100-by-end-of-2022-ecogo-says

Gillespie, P., & Squires, S. (2022, July 28). Argentina Names Third Economy Minister in a Month Amid Crisis. *Buenos Aires Times*. https://www.batimes.com.ar/news/argentina/argentina-names-third-economy-minister-in-a-month-amid-crisis.phtml

Glezer, L. (2021). *El Gobierno apunta a las granjas de Bitcoin por los cortes de luz*. LaPoliticaOnline. Retrieved November 9, 2022, from https://www.lapoliticaonline.com/energia/el-gobierno-le-pide-a-los-grandes-consumidores-de-elecrticidad-que-informen-si-tienen-mineria-de-criptomonedas/

Global Legal Research Center Staff. (2018). *Regulation of Cryptocurrency Around the World*. The Law Library of Congress. https://jolt.richmond.edu/files/2021/02/Bull_cryptocurrency-world-survey.pdf

Global Petrol Prices. (2021, September). Global Control Prices. Electricity Prices. https://www.globalpetrolprices.com/electricity_prices/

Gohwong, S. (2021). Comparative Non-government-based Cryptocurrencies Policy between Thailand and Argentina. *Journal of Contemporary Governance and Public Policy, 2*(2), 122-133. https://doi.org/10.46507/jcgpp.v2i2.44

Government of Argentina. (2001). National Decree 1570/2001. http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70355/norma.htm

Government of Argentina. (2011). General Resolution No. 3210. Administración Federal de Ingresos Públicos. http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/188904/norma.htm

Guadamuz, A., & Marsden, C. (2015). Blockchains and Bitcoin: Regulatory responses to cryptocurrencies. *First Monday*. https://doi.org/10.5210/fm.v20i12.6198

Hughes, E. (1993, March 9). *A Cypherpunk's Manifesto*. https://www.activism.net/cypherpunk/manifesto.html

INDEC (Instituto Nacional de Estadística y Censos). (2021). Mercado de trabajo. Tasas e indicadores socioeconómicos (EPH) [PDF Document]. https://www.indec.gob.ar/uploads/informesdeprensa/mercado_trabajo_eph_4trim211A57838DEC.pdf

Infobae. (2021, November 1). Se renueva el cupo mensual de USD 200: a qué precio vende cada banco y quiénes pueden comprar dólares. https://www.infobae.com/economia/2021/11/01/se-renueva-el-cupo-mensual-de-usd-200-a-que-precio-vende-cada-banco-y-quienes-pueden-comprar-dolares/

International Monetary Fund. (2016). *Virtual Currencies and Beyond: Initial Considerations (IMF Staff Discussion Note)*. https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf

IProfesional (2022, April 20). Renta inesperada: de aprobarse, ya serían 22 los impuestos que se crearon o aumentaron desde 2019. https://www.iprofesional.com/impuestos/360996-los-22-impuestos-que-se-crearon-o-aumentaron-desde-2019

Jamele, A. (2022, July 5). Así fue cómo la renuncia de Martín Guzman precipitó "una estampida crypto" en la Argentina. *Forbes International*. https://www.forbesargentina.com/money/asi-fue-como-renuncia-martin-guzman-precipito-una-estampida-cripto-argentina-n18348

Jarvis, C. (2021). Cypherpunk ideology: Objectives, profiles, and influences (1992–1998). *Internet Histories*, 1-27. https://doi.org/10.1080/24701475.2021.1935547

Katarzyna, C. (2019, March). *Cryptocurrencies: Opportunities, Risks and Challenges for Anti-corruption Compliance Systems.* 2019 OECD Global Anti-corruption & Integrity Forum, Paris. https://www.oecd.org/corruption/integrity-forum/academic-papers/Ciupa-Katarzyna-cryptocurrencies.pdf

Lankes, A. (2022, August 20). Las criptodivisas tropiezan, pero en Argentina son aún una apuesta más segura. *The New York Times*. https://www.nytimes.com/es/2022/08/20/espanol/argentina-bitcoin-criptomonedas.html

Ministry of Economy of the Republic of Argentina. (2022, March 23). *Letter of Intent*. International Monetary Fund. Retrieved January 16, 2023, from https://www.imf.org/-/media/Files/Publications/LOI/2022/ARG030322.ash

Morning Consult. (2022). *The Crypto Report: Our Analysts on the State of Cryptocurrency.* https://go.morningconsult.com/rs/850-TAA-511/images/220630_State_of_Cryptocurrency_Report.pdf

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

Nica, O., Piotrowska, K., & Schenk-Hoppé, K. R. (2017). Cryptocurrencies: Economic benefits and risks. *FinTech Working Paper, 2.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3059856

Olivera Doll, I. (2022, March 15). Argentina to include crypto firms in anti-money laundering regulations. *Buenos Aires Times.* https://www.batimes.com.ar/news/economy/argentina-to-include-crypto-firms-in-anti-money-laundering-regulations.phtml

Reiff, N. (2021, August 26). What's the environmental impact of cryptocurrency? In *Investopedia.* https://www.investopedia.com/tech/whats-environmental-impact-cryptocurrency/

Renieris, E. (2022, March 15). *Crypto's "Freedom to Transact" May Actually Threaten Human Rights*. Centre for International Governance Innovation. https://www.cigionline.org/articles/cryptos-freedom-to-transact-may-actually-threaten-human-rights/

Ro, C. (2022, April 22). Why Argentina is Embracing Cryptocurrency. *BBC*. https://www.bbc.com/news/business-60912789

Rueckert, C. (2019). Cryptocurrencies and fundamental rights. *Journal of Cybersecurity, 5*(1). https://doi.org/10.1093/cybsec/tyz004

Scarpinelli, L. (2015, December). Cepo cambiario: cronología de estos cuatro años de restricciones. *La Nación*. https://www.lanacion.com.ar/economia/cepo-cambiario-cronologia-de-estos-cuatro-anos-de-restricciones-nid1854739/

Schwartz, L., & Idris, A. (2022, May 26). From Argentina to Nigeria, people saw Terra as more stable than local currency. They lost everything. *Rest of World*. https://restofworld.org/2022/argentina-nigeria-terra-crash/

Senado Argentina (2022, May 12). Obtuvo Media Sanción la Creación del Fondo Nacional para la Cancelación de la Deuda con el FMI. *Senado Argentina*. https://www.senado.gob.ar/prensa/20290/noticias

Serrano-Román, A. & Olivera Doll, I. (2022, March 9). Cryptocurrencies Prove a Lifeline in Argentina's Chaotic Economy. *Bloomberg.* https://www.bloomberg.com/news/articles/2022-03-09/cryptocurrencies-prove-a-lifeline-in-argentina-s-chaotic-economy

Sharma, R. (2019, June 25). Hyperinflation Produces Surge in Bitcoin Trading in Venezuela. In *Investopedia*. https://www.investopedia.com/news/hyperinflation-produces-surge-bitcoin-trading-venezuela/

Sier, J., & Hewitt, L. (2022, July 31). What caused crypto to crash this time (in five charts) and will it survive? *Australian Financial Review.* https://www.afr.com/technology/what-caused-crypto-to-crash-this-time-in-five-charts-and-will-it-survive-20220711-p5b0ps

Silverman, J. (2022, March 2). Bitcoin Goes to War. *New Republic*. https://newrepublic.com/article/165559/bitcoin-ukraine-war-cryptocurrency-markets

Slipczuk, M. (2019, August 2). ¿Qué fue la intervención del INDEC y cómo impactó en los datos? *Chequeado*. https://chequeado.com/el-explicador/que-fue-la-intervencion-del-indec-y-como-impacto-en-los-datos/

Slipczuk, M. (2020, September 19). Cronología del cepo cambiario: cómo varió entre 2011 y 2020. *Chequeado*. https://chequeado.com/el-explicador/cronologia-del-cepo-cambiario-como-vario-entre-2011-y-2020/

Smink, V. (2021, December 2). 20 años del "Corralito": 3 cosas que cambiaron en Argentina tras la grave crisis económica, política y social de 2001. *BBC*. https://www.bbc.com/mundo/noticias-america-latina-59494504

Statista. (2022, March). Evolución anual de la tasa de inflación en Argentina desde 2017 hasta 2021. https://es.statista.com/estadisticas/1189933/tasa-de-inflacion-argentina/.

Taquion. (2022). Criptomonedas y Metaverso. El futuro entre nosotros. https://www.taquion.com.ar/wp-content/uploads/2022/04/TAQUION-DOSSIER-CRIPTOMONEDAS-Y-METAVERSO-Abr-22.pdf

Valkyrie Invest. (2021). *Part II: LatAm Bitcoin Adoption*. https://valkyrieinvest.com/wp-content/uploads/2021/09/Valkyrie-The-Bitcoin-Effect-Part-2.pdf

Van Valkenburgh, P. (2015). *Bitcoin: Our Best Tool for Privacy and Identity on the Internet.* Coin Center. http://coincenter.org/2015/03/bitcoin-our-best-tool-for-privacy-and-identity

Van Valkenburgh, P. (2019). *Electronic Cash, Decentralized Exchange, and the Constitution 1.0.* Coin Center. https://www.coincenter.org/app/uploads/2020/05/e-cash-dex-constitution.pdf

Cutting-Edge Technologies in Developing Economies: The Case of India's Semiconductor Industry

Andreas Kuehn and Trisha Ray

ABSTRACT:

This paper analyzes the Government of India's spate of new semiconductor government policies and industry initiatives to establish and grow the national semiconductor ecosystem. It does so against the backdrop of both the country's own history with semiconductors, starting in the 1950s, as well as geopolitical narratives on reducing foreign supply dependencies, and the emergence of gated globalization. The paper highlights five factors to measure the success of India's policies and provide learnings for emerging economies embarking on similar high-tech policy efforts: improving bureaucratic expediency; securing international partners; managing stress on basic infrastructure and resources; filling gaps in semiconductor talent; and enhancing the country's relative competitiveness among developing digital economies.

KEYWORDS: Semiconductors; digital transformation; microchips; global value chains; electronics manufacturing; India; talent; reshoring.

1 INTRODUCTION

Semiconductors are critical components to a country's digital transformation. Yet most economies must satisfy their chip demand from technologically advanced countries and blocs such as the United States, China, the Netherlands, Japan, South Korea, and Taiwan.[1] This is further complicated by the fact that semiconductor supply chains are heavily bottlenecked; global in scale yet geographically concentrated, semiconductor design and production require significant financial investments and highly specialized knowledge, infrastructure, and talent. The industries of emerging countries have historically not succeeded in developing any meaningful capacities due to the lack of necessary resources, capabilities, and conditions to manufacture cutting-edge technologies. Their role has been relegated to low-value suppliers at best, if they were integrated into the global technology supply chain at all.

The Indian government has initiated a new semiconductor manufacturing program with significant budgetary allocations, but it has yet to address the multifaceted policy, economic, environmental, and technological challenges for a developing economy to break into the production of high-tech technologies, ranging from significant financial investments, talent, critical energy and water infrastructure, and integration into the global supply chain. To examine the policies and their challenges, the paper draws from in-depth, off-the-record expert interviews with current and former government officials, trade associations, industry decision-makers, and technology experts, as well as a systematic document analysis of publicly available government and corporate documents. The inquiry focuses on the history and current policy efforts to establish India as a semiconductor hub. Our analysis of these efforts finds five major factors that will determine the success of India's semiconductor push, which in turn could provide direction for other developing economies with comparable policy pursuits:

1. Strong policy direction, as well as bureaucratic expediency to leverage ongoing "reshoring" of supply chains.
2. The pivotal role of partnerships with established semiconductor design and manufacturing hubs like the United States, the Netherlands, Taiwan, South Korea, or Japan.
3. Managing competing demands for basic infrastructure, like water and electricity, which directly impact the quality of life of citizens.
4. Leveraging existing (and abundant) semiconductor design talent in India, while also working on a strategy to acquire and develop skilled labor in other areas of semiconductor fabrication and facilities design.
5. How the combination of the above four factors helps position India vis-à-vis other developing economies that are already angling themselves as competitive alternatives to China for reshoring.

2 HISTORY

At the time of its independence in 1947, India had undergone nearly two centuries of "deindustrialization" under the British Raj (Bagchi, 1976). India's early post-independence technology policies are reminiscent of its current focus on *Aatmanirbhar Bharat* (self-reliant India).[2] This early focus, according to some accounts (Sukumar, 2019, pp. 9-11), was driven largely by Jawaharlal Nehru's emphasis on "scientific temper," or an understanding of the technologies being used, rather than technology being deployed for its own sake. [3]

In the 1960s, a handful of Indian companies were producing germanium semiconductors. Bharat Electronics Ltd. (BEL), a public sector undertaking (PSU) under the Ministry of Defense (MoD), acquired germanium and silicon technology for producing semiconductor devices. The semiconductor industry in India picked up pace in the 1980s when the government relaxed some licensing requirements and lifted import duties on computers and other electronic equipment. Then in 1984, the government established Semiconductor Complex Ltd. (SCL), a PSU formed through licensing agreements with Hitachi, AMI, and Rockwell. Additionally, the government invited bids to set up a National Silicon Facility (NSF), which saw considerable interest from companies in the United States and Germany.[4] Eventually, the newly formed Metkem Silicon Ltd., an Indian company, set up its polysilicon facilities with support from BEL.

1 India, for instance, imports 100%, or $24 billion worth of semiconductors annually (as of 2021), a number which is estimated to grow to $100 billion by 2025 (Chauhan, 2022).

2 India's current focus on self-reliance has a long history. The Swadeshi movement, a pre-Independence movement to boycott British goods, is an example, as are all its Five-Year Plans since 1947.

3 Indeed, Nehru's early encounters with American industrialists elicited much the same response as India's modern industrial policies. As then-U.S. ambassador Stephen Grady said, "Indian friends seemed to think American know-how can be shipped to them in sealed cases laid down at Indian ports" (Sukumar, 2019).

4 The NSF was not without controversy. Hemlock Semiconductors, an American company, was initially chosen as a partner by the Department of Electronics. However, the initial outlay of ₹200 was deemed as too high by the Department of Non-conventional Energy Sources (DNES), which supported a domestic alternative instead, namely IISc-MCIC. (Public Accounts Committee, 1989)

In the decades since the 1990s, India's semiconductor efforts have floundered. The SCL complex in Chandigarh was razed in a fire in 1989, and while it was eventually revived, it only produced a small number of chips for the Indian Space Research Organization (ISRO). Further, India's economic liberalization policies starting in 1991 resulted in an uptick in (now cheaper) semiconductor imports. Together with the lack of promised government subsidies, especially for electricity, these factors chipped away at India's fledgling semiconductor manufacturing ecosystem in the subsequent decade.

In 2007, the government announced it was working on the country's first Semiconductor Policy, to attract ₹24,000 (approximately $3.1 billion)[5] of investment over three years, along with three fabrication (fab) units. In this period, AMD and Intel were both considering setting up fabs in India ("India Snoozed, Lost Intel Chip Plant," 2007). Both failed to take root, however, due to a variety of factors: the delay in both the passage and the implementation of the Semiconductor Policy as well as its stringent minimum investment requirement for qualifying for incentives, fundraising issues, and production delays (Arakali, 2008). In 2013–14, the government tried to revive its semiconductor push, issuing letters of intent (LOIs) to two consortiums—Hindustan Semiconductor Manufacturing Corporation (STMicroelectronics and SilTerra Malaysia Sdn. Bhd.) and Jaiprakash Associates Ltd. (IBM and Tower Semiconductor Ltd)—both of which failed to materialize.

The history of India's semiconductor policies provides a few key lessons: government interventions need to be both strategic and timely. By the end of the 1980s, India was—according to commentators—just two years behind the latest semiconductor manufacturing technologies (Shivaram, 2022). The government's role in easing regulations and reaching out to investors, while supporting homegrown enterprises, had been pivotal. Yet it was India's bureaucracy that eventually became a barrier: the lack of coordination between relevant ministries and government agencies, the slowness of policies and grants, and the absence of supporting infrastructure all led to the country falling decades behind.[6]

3 AATMANIRBHAR BHARAT: India Revives its Semiconductor Ambitions

The U.S.-China trade war and the lack of a coordinated global response to COVID-19 have re-imprinted in the minds of Indian policymakers the inextricable relationship between geopolitics and access to technology. Supply chains are necessarily global—for reasons of efficiency—but are considered security risks, with states investing in capacities, capabilities, rules, and institutions to reduce foreign reliance and protect domestic innovation and comparative economic and strategic advantage. India's Minister of External Affairs, S. Jaishankar, describes this phenomenon: "[T]he big takeaway from COVID, to me, is an argument for shorter supply chains, more national capacities, and I've always felt we have neglected the domestic supply chains and deeper strengths … people have had to accept that, national competition, advancement of national ambitions, all these things are very much a reality, despite economic globalization" (Haidar, 2021).

The simultaneous focus on domestic self-reliance and global competitiveness represents India's response and ambition to an emergent trend, namely, "gated globalization," where nations and blocs are becoming more selective about the partners they choose to trade with, sometimes based on nebulous concepts like "like-mindedness" (Khar, 2016; Sinha & Saran, 2020). The strategic security dialogue between India and the United States, Japan, and Australia, i.e., the Quad, addresses semiconductors as a critical and emerging technology and serves as an example of that development. Leaders in the Indian government have often highlighted geopolitical and techno-nationalist narratives when inviting investments into the country's electronics and telecommunications sector (Ray, 2022; "India can bring trusted solutions for the world," 2022).

The simultaneous focus on domestic self-reliance and global competitiveness represents India's response and ambition to an emergent trend, namely, "gated globalization."

To lessen supply chain dependencies on foreign technology suppliers, the Modi government added *Aatmanirbhar Bharat*, or "self-sufficient India," to its policy lexicon. In this vein, India has set out to establish its own semiconductor industrial base. India imports all its semiconductors (Srivastava, 2021), valued at approximately $15 billion in 2020 (Tripathy & Thirukarugavur, 2021). The India Electronics and Semiconductor Association (IESA) estimates the country's semiconductor consumption at $21 billion (as of 2019) with a growth rate of 15.1% (India Electronics and Semiconductor Association, n.d.). Meanwhile, a total of $2.5 billion in revenue was generated from semiconductor research and development in India, where more than 90% of semiconductor companies have research and development centers (Singal, 2020). Despite this, however, India lags far behind leaders like the United States, Taiwan, South Korea, Japan, and Singapore as well as China when it comes to semiconductor manufacturing.

The breakdown of supply chains and the consequent semiconductor shortage in the period starting in 2021 led to the stagnation or decline of India's automotive industry and production of telecommunications equipment (Ministry of Finance, 2022). Port delays, higher freight rates, and a shortage of shipping containers are other concerns that factor into the government's thinking on managing supply chain issues.

To enhance India's position in the global semiconductor landscape but also to satisfy the demands of India's domestic microelectronics industry, government policies in recent years have aimed at establishing and growing semiconductor manufacturing capacity (i.e., fabs). In April 2020, the government announced three schemes to promote India's semiconductor industry, with a total outlay of ₹50,000 (approximately $6.5 billion). Then, in December 2021, the Government of India approved the Semicon India Program and dedicated ₹76,000 (approximately $10 billion) over six years to develop the country's semiconductor ecosystem (Ministry of Electronics and Information Technology, 2021). The program will support entities working on silicon semiconductors, display fabs, compound semiconductors/silicon photonics/sensors, semiconductor packaging, and semiconductor design. Semicon India will cover significant parts of the industry's initial investments and operating costs during the program's lifetime. The Semicon India program includes the establishment of 20 manufacturing units and will provide incentives both to existing large companies and to startups and small companies that are looking to design and manufacture semiconductors (Cyrill & Kapur, 2022). For new fabs in India, eligible companies can receive up to 50% of their set-up and operating costs and product deployment-linked incentives of 4–6% on net sales for five years (Singal, 2021). As part of this incentive program, the government is also planning to train semiconductor engineers.

5 Based on May 2022 exchange rates.

6 In a similar vein, China's government has been attempting to establish a domestic semiconductor industry. Its strategic central plans and government interventions for a homegrown semiconductor ecosystem experienced a similar fate and has recently been complicated by U.S. and international Western responses to the growing technology competition in critical and emerging technology. For an account of China's semiconductor policy developments, see Xiang (2021).

TABLE 4. Summary of India's semiconductor policies (2015–2022)

POLICY	KEY PROVISIONS	BUDGET ALLOCATED	IMPLEMENTING BODY
Scheme for Promotion of Manufacturing of Electronic Components and Semiconductors (SPECS)[7] 2020–2025	Financial incentive of 25% on capital expenditure for electronic goods that comprise the downstream value chain of electronic products. Applicable to both new units and expansion of existing capacities. Projects must meet a minimum investment threshold to qualify.	₹50,000 ($6.7 billion approx.)	Designated Project Management Agency (Under the Ministry of Electronics and Information Technology, MeitY)
Modified Electronics Manufacturing Clusters (EMC 2.0) Scheme[8] 2020–2025	Supports electronics manufacturing with the aim of greater integration into global value chains (GVCs). Financial assistance up to 50% of project costs (capped at ₹70 for 100 acres of land). Covers basic infrastructure costs, essential services, employee welfare facilities, business development services, and manufacturing support.		Designated Project Management Agency (Under MeitY)
Production-Linked Incentives (PLIs) for Large Scale Electronics Manufacturing[9] 2020–2025	Incentive of 4–6% on incremental sales (over a base year) of goods manufactured in India for five years.		Empowered Committee (EC) of high-level representatives of government agencies (under guidance from MeitY)
Semicon India Program[10] 2022–2028	Fiscal support for semiconductor companies developing and producing components. Offsets of 50% of operating costs for setting up semiconductor manufacturing units.	₹76,000 ($10 billion approx.)	India Semiconductor Mission (ISM is a division of the Digital India Corporation, which in turn is under MeitY.)

7 (Ministry of Electronics and Information Technology, 2022b).

8 (Ministry of Electronics and Information Technology, 2020a).

9 (Ministry of Electronics and Information Technology, 2020a).

10 (Ministry of Electronics and Information Technology, 2021).

POLICY	KEY PROVISIONS	BUDGET ALLOCATED	IMPLEMENTING BODY
Electronics Development Fund (EDF)[11] 2015–2017	"Fund of funds" provides risk capital to companies developing new technologies in electronics, nanoelectronics, and information technology. Aims to build domestic IP in the areas mentioned above. EDF supports "daughter funds" at Indian VCs.	₹359 ($46 million approx.)	Fund manager: CANBANK Venture Capital Funds Anchor investor: MeitY

By February 2022, India's government had received proposals under Semicon India from Indian and international companies. This included proposals from industry behemoth Taiwan Semiconductor Manufacturing Company Ltd (TSMC); India's Tata Group, which plans to invest up to $300 million to set up a semiconductor assembly and test unit (Pradeep, 2021); a Vedanta (India)-Foxconn (Taiwan) joint venture; IGSS Ventures (Singapore); and ISMC[12] (Swarajya Staff, 2022; Vengattil, 2022).

4 INTERNATIONAL EFFORTS TO STRENGTHEN SEMICONDUCTOR CAPACITIES

India's semiconductor policies come at a pivotal moment. To strengthen national technology independence and build up domestic capacities but also to curb China's access to critical components in semiconductor development and production, the United States and like-minded countries have initiated efforts to reshape global semiconductor supply chains. Current dependence on foreign key technology components and tensions with China over Taiwan, the central fabrication hub for semiconductors globally, are major drivers of reshoring. Countries have all experienced how access to microchips is central not just to their digital transformation, but to economic and military power as well. Shortages in the period starting in 2020 have held back industry output in the automotive and appliance sectors. More acutely, the Russian invasion of Ukraine underscored the importance of microelectronics for warfighting, but it also has the potential to further disrupt semiconductor supply (Gauthier-Villars et al., 2022; Pollet, 2022).

The U.S. government blocked the sale of critical components and equipment through tightened export control rules to Chinese technology firms and chip manufacturers, at a significant cost to the U.S. industry. To secure U.S. semiconductor leadership, Congress has passed the CHIPS and Science Act, a close to $53 billion investment plan to promote domestic semiconductor research, design, and manufacturing (Semiconductor Industry Association, 2022). The EU aims at doubling its global market share to at least 20% by 2030 through the European Chips Act. These efforts are accompanied by outreach to international partners. Semiconductors are high on the agenda of the Quad, the U.S.-EU Trade and Technology Council, and the Chip 4 compact between the U.S., South Korea, Japan, and Taiwan, which represent new forms of technology alliances that are emerging to manage strategic technology competition vis-à-vis adversaries.

In the Indo-Pacific, Vietnam and Malaysia are both strong contenders in attracting international semiconductor investments

11 (Ministry of Electronics and Information Technology, 2020b).

12 ISMC is a $3 billion joint venture between Abu Dhabi-based Next Orbit Ventures and Israel's Tower Semiconductor to establish a semiconductor fab in India's southern state of Karnataka.

from the United States' reshoring efforts. The Vietnamese government has successfully prioritized the electronics and semiconductor industry through the years, including through the "National program for high-tech development until 2020," and the list of national products implemented from 2012 under the National Product Development Program to 2020. The policies helped catapult Vietnam into a top electronics exporter within the past ten years (Dezan Shira & Associates, 2021; Luu, 2021). Vietnam's semiconductor industry is expected to grow at almost 19% CAGR, or $6.16 billion from 2020 to 2024 (Chen & Hu, 2021). Vietnam has leveraged free trade agreements, deployed corporate tax breaks, and created high-tech industrial zones; in addition, its demographic structure, labor qualifications, and regionally competitive wages are attractive to semiconductor investments (Nguyen, 2020). Like India, though, Vietnam is dominated by foreign players and has yet to integrate into the global market and move up in the semiconductor value chain (Dezan Shira & Associates, 2021). Malaysia, on the other hand, already has a mature semiconductor industry, cutting across chip design, manufacturing, packaging, and testing, and is considered ASEAN's semiconductor hub. It accounts for 7% of the global chips trade and contributes about 13% of global back-end capacity (assembly, test, and packaging of chips), operated by the likes of Intel, Micron, and Texas Instruments, from which Malaysia has repeatedly attracted investments to grow its national semiconductor base (Kaur, 2021; Tieying, 2021). According to observers, Malaysia is well positioned to move further up the value chain in the long term (Tieying, 2021).

For India, this larger context means two things. First, with the United States reshoring its semiconductor supply chains, there is an opportunity to become the destination of choice for these reshaped supply chains as international semiconductor firms move their chip operations out of China.[13] At the same time, India faces the chicken-and-egg problem of establishing connections with suppliers and buyers beyond its domestic electronics industry and integrating into the global chips ecosystem, but will likely only triumph after proving that its new policies have successfully established a competitive semiconductor hub.[14] Second, India at the same time faces stiff competition from established and emerging semiconductor hubs like Singapore, Vietnam, and Malaysia in Southeast Asia, as well as China and, to a far lesser degree, European efforts.

5 OUTLOOK, PECULIARITIES, AND RECOMMENDATIONS

India has started a commendable undertaking to build up its domestic semiconductor industry to sustain its own domestic demands, ensure supply reliability for its electronics and automotive sectors, and move up in the value chain. At present, India's semiconductor demand is around $24 billion, but by 2025 it is expected to be $100 billion. It remains to be seen whether the government's initiatives will overcome the traditional obstacles of bureaucracy and red tape.

In the short term, the level of investment provided by the Indian state is unlikely to sustain the development of expensive leading-edge chips fabrication capacities. In fact, current supply chain relocation from China to India in the electronics sector is focused on assembly (Kharpal, 2022). Industry experts have, in this line, recommended that India focus its investments on assembly, testing, marking, and packaging (ATMP) (Banerjee, 2021; Observer Research Foundation, 2022b). ATMP, which is part of the back-end process of chip manufacturing, is characterized by lower capital expenditure, bigger added value, and higher R&D and labor intensity, fitting India's strength and talent pool in the chips industry. Strong packing capabilities, for example, could help relocate functions executed elsewhere, and in the long run, bring India a step closer to chip fabrication.[15]

13 A Ministry of External Affairs official interviewed for this paper placed particular emphasis on the need for India to capitalize on this shift, mostly of testing and assembly facilities, out of China. It should be noted, though, that this is not part of India's official semiconductor policy but rather a timely, opportunistic move to take advantage of the changing semiconductor landscape.

14 Based on interviews with an industry expert and a supply chain analyst.

15 Based on interviews with semiconductor industry analysts.

The right business environment and workforce are key factors for the success of India's chips policy. In comparison to other national efforts, India is peculiar in that it has no shortage of skilled workers and top-tier talent, yet has struggled to realize its ambition of setting up a domestic fab. A 2011 report by Ernst & Young noted India's globally competitive design industry but cited the lack of a manufacturing ecosystem, as well as a shortage of highly specialized skills that could afford a greater role in global value chains, as major challenges (India Semiconductor Association, 2011).

In comparison to other national efforts, India is peculiar in that it has no shortage of skilled workers and top-tier talent, yet has struggled to realize its ambition of setting up a domestic fab.

India's domestic design talent pool comprises one-fifth of the world's semiconductor design engineers, a workforce of about 25,000 engineers working on chip design and verification ("Making India Semiconductor Hub," 2022; Vanamali, 2021; Jaishankar, 2022). Outside of India, Indian-born high-skilled technical workers are a significant part of the semiconductor workforce and account for 21,800 high-skilled technical workers (10%) in the United States (Hunt & Zwetsloot, 2020). Daly (2020) writes, "Despite having extensive top talent, India's chip sector remains essentially a 'design services job shop.' Global multinationals leverage Indian expertise at low cost while capturing the IPR and attendant profits." Recognizing the importance of India's talent pool for the country's domestic semiconductor base is crucial. To that end, the Chips-to-Startup program aims at training 85,000 semiconductor engineers, providing the needed workforce to attract the necessary investments for India's domestic end-to-end semiconductor value chain (Duggal, 2021).

India's current policy envisions a future semiconductor industry that leverages its domestic talent pool and focuses on the cutting-edge design of next-generation chips (e.g., for specialized artificial intelligence applications) that are both *designed* and *fabricated* in India. It does not however, envision a fabless alternative, in which fabrication is outsourced to a foundry elsewhere. India should consider leveraging its large and globally significant design workforce as it maintains a leading position in semiconductor talent. In particular, India should consider EDA (electronic design automation) tools. A focus on developing EDA tools would leverage India's existing semiconductor human capital while reducing dependence on foreign tools. Leading EDA tools developers are present in several Indian cities, which, in collaboration with leading Indian universities, could be turned into native advancement in this area.

Building up a semiconductor base in emerging economies comes with challenges, however, which are especially pronounced over competing industrial interests versus societal needs over infrastructure and resources. Water scarcity has become a challenge to the semiconductor industry in Taiwan, for example, as competing industrial, agriculture, and societal needs must be managed (Huang & Chang, 2022). Throughout the last decade, leading semiconductor manufacturers, including Taiwan Semiconductor Manufacturing Company and Intel, have been faced with water scarcity issues (Johnson, 2022), and this will be a particular challenge for India as well. The expansion of India's semiconductor sector necessitates a capable infrastructure for advanced manufacturing, including reliable water and power infrastructure. These investments in the digital transformation, specifically the semiconductor sector, could be at odds with the needs of India's population and cause societal tensions. India is among the world's most water-stressed nations and has experienced severe water shortages while concurrently experiencing an energy crisis (World Bank Group, 2022;

Mukharji, 2021). Chip factories are estimated to consume up to 20 million liters of water a day, although water recycling technologies have reduced the amount of nonrenewable groundwater needed (Vanamali, 2021; Y, 2022). About 78% of India's freshwater resources are used in agriculture (Kumar, 2021). Establishing semiconductor manufacturing facilities in India, therefore, calls for better water management while meeting the drinking, domestic, and irrigation water requirements. India's national water policy tries to address some of these issues by promoting sustainable and rational use of water.[16] States play a vital role in semiconductor policy implementation, as water and other regulatory domains are a state matter. To that end, states with competitive water and/or power resources, including the states of Telangana, Andhra Pradesh, and Himachal Pradesh, can or have offered incentive packages based on those resources to attract semiconductor investments.[17]

Finally, and crucially, India's actions in the semiconductor space must be contextualized and assessed against current geopolitical dynamics and growing international security tensions. Its choice of partnerships must navigate the headwinds of geopolitical competition between the United States and China, as well as India's own role in a network of technology coalitions of the like-minded. Minister of State for Electronics and Information Technology Rajeev Chandrasekhar, at the CyFy 2022 conference in New Delhi, has emphasized the need for democracies to work together on critical and emerging technologies (Observer Research Foundation, 2022a). At the same time, New Delhi is wary of restrictive U.S. export controls and policies, and is acting to shield itself from the fallout of this trend toward gated globalizati

6 CONCLUSION

India's semiconductor ambitions have, in the course of its history, faced setbacks arising from a combination of construction and production delays, lack of interministerial coordination, and bureaucratic paperwork. The Government of India's recent semiconductor policies, encompassing varied incentives for both Indian and foreign firms, indicate will on the part of political leadership to support the growth of the country's commercial semiconductor manufacturing, assembly, and testing industries. While it is still too early to assess the success of these efforts, observers and policymakers in India as well as other countries hoping to embark on a similar push to move up high-tech value chains should track progress in certain parameters, including improving bureaucratic expediency, securing international partners, managing the stress on basic infrastructure and resources, and filling gaps in semiconductor talent.

16 Some states, such as Gujarat, have addressed water management issues by forming Water and Sanitation Management Organizations (WASMOs), which work in close collaboration with village-level institutions to do efficient water management (Water and Sanitation Management Organization, n.d.).

17 Based on interviews with policy analysts.

REFERENCES

Arakali, H. (2008, February 19). SemIndia Inc to delay India plant by 3 yrs. *Mint.* https://www.livemint.com/Companies/6MLh17Qa14UmQzMefEPwAN/SemIndia-Inc-to-delay-India-plant-by-3-yrs.html

Bagchi, A. K. (1976). De-industrialization in India in the nineteenth century: Some theoretical implications. *The Journal of Development Studies, 12*(2), 135-164. https//doi.org/10.1080/00220387608421565

Banerjee, P. (2021, June 9). India's journey in chip-making may start with ATMPs. *Mint*. https://www.livemint.com/technology/tech-news/indias-journey-in-chip-making-may-start-with-atmps-11623259001571.html

Chauhan, S. (2022, January 11). India's chase to the semiconductor business, strangleholds and up comings. *ELE Times*. https://www.eletimes.com/indias-chase-to-the-semiconductor-business-strangleholds-and-up-comings

Chen, A., & Hu, Y. (2021, August 16). Vietnam's semiconductor industry expected to reach US$6.16 billion in 2024. *DigiTimes*. https://www.digitimes.com/news/a20210813PD214.html

Cyrill, M., & Kapur, Y. (2022, February 21). *Setting Up a Semiconductor Fabrication Plant in India: What Foreign Investors Should Know*. India Briefing. Retrieved June 30, 2022, from https://www.india-briefing.com/news/setting-up-a-semiconductor-fabrication-plant-in-india-what-foreign-investors-should-know-22009.html

Daly, T. (2020, August 13). *Should India Invest in Semiconductor Manufacturing?* SemiWiki. Retrieved June 30, 2022, from https://semiwiki.com/semiconductor-manufacturers/289461-should-india-invest-in-semiconductor-manufacturing/

Dezan Shira & Associates. (2021, July 2). Q&A: Electronics and Semiconductor Industry in Vietnam. *Vietnam Briefing*. https://www.vietnam-briefing.com/news/qa-electronics-and-semiconductor-industry-in-vietnam.html

Duggal, S. (2021, December 15). India to create a pool of 85000 high-skilled engineers under chips to startups. *The Economic Times*. https://economictimes.indiatimes.com/jobs/india-to-create-a-pool-of-85000-high-skilled-engineers-under-chips-to-startups/articleshow/88297718.cms

Gauthier-Villars, D., Stecklow, S., & Shiffman, J. (2022, April 29). *How military technology reaches Russia in breach of U.S. export controls.* Reuters. https://www.reuters.com/world/how-military-technology-reaches-russia-breach-us-export-controls-2022-04-29

Haidar, S. (2021, December 14). Jaishankar bats for domestic production over unchecked globalisation. *The Hindu*. https://www.thehindu.com/news/national/jaishankar-bats-for-domestic-production-over-unchecked-globalisation/article37955457.ece

Huang, W.-C., & Chang, C.-W. (2022). Water shortage risk in Taiwan's Silicon Valley. *Journal of the Chinese Institute of Engineers 45*(6), 513-520. https//doi.org/10.1080/02533839.2022.2078420

Hunt, W., & Zwetsloot, R. (2020, September). *The Chipmakers: U.S. Strengths and Priorities for the High-End Semiconductor Workforce* [CSET Issue Brief]. CSET. https://cset.georgetown.edu/wp-content/uploads/CSET-The-Chipmakers.pdf

India can bring trusted solutions for world; first semiconductor project approval this year: Ashwini Vaishnaw. (2022, June 26). *Economic Times*. https://economictimes.indiatimes.com/news/india/india-can-bring-trusted-solutions-for-world-first-semiconductor-project-approval-this-year-ashwini-vaishnaw/articleshow/92472677.cms

India Electronics and Semiconductor Association. (n.d.). *India Electronics and Semiconductor Association (IEAS)*. https://iesaonline.org

India Semiconductor Association. (2011). *Study on semiconductor design, embedded software, and services industry*. https://www.meity.gov.in/writereaddata/files/Semiconductor06April11_020511.pdf

India Snoozed, Lost Intel Chip Plant. (2007, September 6). *Forbes*. https://www.forbes.com/2007/09/06/intel-india-china-markets-equity-cx_rd_0906markets1.html?sh=3390c3bc4bf9

Jaishankar, D. (2022, October 18). India plays a crucial role in US semiconductor plans. *Hindustan Times*. https://www.hindustantimes.com/opinion/india-plays-a-crucial-role-in-us-semiconductor-plans-101666100297706.html

Johnson, D. (2022, January 25). Scarcity Drives Fabs to Wastewater Recycling. *IEEE Spectrum*. https://spectrum.ieee.org/fabs-cut-back-water-use

Kaur, D. (2021, October 6). For Taiwan, Malaysia could ease the global semiconductor shortage. *Tech Wire Asia*. https://techwireasia.com/2021/10/for-taiwan-malaysia-could-ease-the-global-semiconductor-shortage/

Khar, H. R. (2016). Gated globalization. In *Connectivity Wars* (p. 4). European Council on Foreign Relations. https://www.jstor.org/stable/pdf/resrep21667.14.pdf

Kharpal, A. (2022, September 26). Apple begins making the iPhone 14 in India, marking a big shift in its manufacturing strategy. *CNBC*. https://www.cnbc.com/2022/09/26/apple-starts-manufacturing-the-iphone-14-in-india.html

Kumar, M. J. (2021). Is India going to be a major hub of semiconductor chip manufacturing? *IETE Technical Review, 38*(3), 279-281. https://doi.org/10.1080/02564602.2021.1916166

Luu, D. (2021, May 19). Great opportunity for Vietnam's semiconductor industry. *Vietnamnet*. https://vietnamnet.vn/en/great-opportunity-for-vietnams-semiconductor-industry-726566.html

Making India Semiconductor hub. (2022, May 1). *The Statesman*. https://www.thestatesman.com/business/making-india-semiconductor-hub-1503066456.html

Ministry of Electronics and Information Technology, Government of India. (2020a, April 1). *Modified Electronics Manufacturing Clusters (EMC 2.0) Scheme* [Notification]. https://www.meity.gov.in/writereaddata/files/modified_electronics_manufacturing_clusters_scheme.pdf

Ministry of Electronics and Information Technology, Government of India. (2020b, July 15). *Electronics Development Fund (EDF) policy*. Retrieved June 30, 2022, from https://www.meity.gov.in/esdm/edf

Ministry of Electronics and Information Technology, Government of India. (2021, December 23). *Programme for Development of Semiconductors and Display Manufacturing Ecosystem in India | Ministry of Electronics and Information Technology, Government of India*. Retrieved June 30, 2022, from https://www.meity.gov.in/content/programme-development-semiconductors-and-display-manufacturing-ecosystem-india

Ministry of Electronics and Information Technology, Government of India. (2022a, March 14). *Production Linked Incentive Scheme (PLI) for Large Scale Electronics Manufacturing*. Retrieved June 30, 2022, from https://www.meity.gov.in/esdm/pli

Ministry of Electronics and Information Technology, Government of India. (2022b, April 1). *Scheme for Promotion of Manufacturing of Electronic Components and Semiconductors*. Retrieved June 30, 2022, from https://www.meity.gov.in/esdm/SPECS

Ministry of Finance. (2022, January 31). *Economic Survey (2021-2022)*. https://www.indiabudget.gov.in/economicsurvey/

Mukharji, A. (2021, October 11). Why India is on the brink of an unprecedented power crisis. *BBC*. https://www.bbc.com/news/business-58824804

Nguyen, T. (2020, July 24). Vietnam's Electronics Industry: A Guide to Emerging Opportunities. *Vietnam Briefing*. https://www.vietnam-briefing.com/news/vietnams-electronics-industry-guide-emerging-opportunties.html/

Observer Research Foundation (2022a, October 26). Democracies Need to Work Together; US Has Reached A Late But Correct Approach On China. *YouTube*. https://www.youtube.com/watch?v=pqgq7ee8xeM

Observer Research Foundation (2022b, October 27). Down to the Nanometer: Chasing the Semiconductor Windfall. *YouTube*. https://www.youtube.com/watch?v=j8kjy60eog4

Pollet, M. (2022, March 7). Ukraine war could further disrupt semiconductor production. *EURACTIV.com*. https://www.euractiv.com/section/digital/news/ukraine-war-could-further-upset-the-production-of-semi-conductors/

Pradeep, N. S. (2021, November 28). The $300 million dollar semiconductor project: The TATA Group's proposal in setting up of semiconductors in three states. *fanaticbuff*. https://fanaticbuff.com/the-300-million-dollar-semiconductor-project-the-tata-groups-proposal-in-setting-up-of-semiconductors-in-three-states/

Public Accounts Committee (1988-89). (1989, April 28). *National Silicon Facility* (Issue Hundred and Fifty-Eighth Report). Department of Electronics. https://eparlib.nic.in/bitstream/123456789/5129/1/pac_8_158_1989.pdf

Ray, T. (2022, June 1). *The Quad and the wicked problem of tech standards*. Observer Research Foundation. https://www.orfonline.org/expert-speak/the-quad-and-the-wicked-problem-of-tech-standards/

Semiconductor Industry Association. (2022). *CHIPS for America Act & FABS Act*. Retrieved June 30, 2022, from https://www.semiconductors.org/chips/

Shivaram, C. (2022, February 17). India's semiconductor moment. *The Statesman*. https://www.thestatesman.com/opinion/indias-semiconductor-moment-1503046515.html

Singal, N. (2020, August 31). No big investment in semiconductor manufacturing recently, but interest rises: Industry body. *Business Today*. https://www.businesstoday.in/latest/corporate/story/no-big-investment-in-semiconductor-manufacturing-recently-but-interest-rises-industry-body-271653-2020-08-31

Singal, N. (2021, December 15). Govt's roadmap to make India hub of semiconductor manufacturing. *Business Today*. https://www.businesstoday.in/latest/economy/story/govts-roadmap-to-make-india-hub-of-semiconductor-manufacturing-315701-2021-12-15

Sinha, J., & Saran, S. (2020, April 27). Gated globalisation and fragmented supply chains. *The Economic Times*. https://economictimes.indiatimes.com/news/international/business/view-nations-may-opt-to-trade-with-economies-where-political-trust-exists-thereby-fragmenting-supply-chains/articleshow/75395926.cms?

Srivastava, S. (2021, December 21). *India Sees Chipmakers Starting Local Production in 2-3 Years*. Bloomberg.com. https://www.bloomberg.com/news/articles/2021-12-22/india-sees-chip-makers-starting-local-manufacturing-in-2-3-years

Sukumar, A. M. (2019). *Midnight's Machines: A Political History of Technology in India*. Penguin Random House. https://penguin.co.in/book/midnights-machines/

Swarajya Staff. (2022, February 20). Here Is What We Know So Far About the Applicants for India's $10 Billion Incentive Scheme for Semiconductors. *Swarajya*. https://swarajyamag.com/analysis/here-is-what-we-know-so-far-about-the-applicants-for-indias-10-billion-incentive-scheme-for-semiconductors

Tieying, M. (2021, September 23). *ASEAN's potential in semiconductor manufacturing*. DBS. https://www.dbs.id/id/personal/templatedata/article/generic/data/en/GR/092021/210923_insights_semiconductor.xml

Tripathy, A., & Thirukarugavur, H. (2021, June 28). How To Lay the Solid Foundation for Semiconductor Fabrication in India. *Forbes India*. https://www.forbesindia.com/article/iim-bangalore/how-to-lay-the-solid-foundation-for-semiconductor-fabrication-in-india/68795/1

Vanamali, K. V. (2021, December 17). Will India be able to attract global chipmakers with $10 bn incentive. *Business Standard*. https://www.business-standard.com/podcast/current-affairs/will-india-be-able-to-attract-global-chipmakers-with-10-bn-incentive-121121700069_1.html#

Vengattil, M. (2022, May 1). *Chip consortium ISMC to set up $3 billion plant in India's Karnataka*. Reuters. https://www.reuters.com/world/india/chip-consortium-ismc-plans-3-bln-plant-indias-karnataka-2022-05-01

Water and Sanitation Management Organization. (n.d.). *Water and Sanitation Management Organization*. Retrieved June 30, 2022, from https://wasmows.gujarat.gov.in/

World Bank Group. (2022, March 14). *World Water Day 2022: How India is addressing its water needs.* https://www.worldbank.org/en/country/india/brief/world-water-day-2022-how-india-is-addressing-its-water-needs

Xiang, N. (2021). *US-China Tech War: What Chinese Tech History Reveals about Future Tech Rivalry.* Independently Published.

Y, J. (2022, March 9). The Big Semiconductor Water Problem. *The Asianometry Newsletter.* https://asianometry.substack.com/p/the-big-semiconductor-water-problem

International Governance of New Technologies

Standards Makers and Standards Takers: Geopolitics, Emerging Countries, and the Future of Technology Governance

Julia Voo

ABSTRACT:

The role of emerging countries in shaping future technology governance has been overlooked. In response to the U.S.-China technology competition, technical standards and technology governance have been identified as key areas of Chinese influence that the U.S. and its allies have prioritized. However, the U.S. and its allies have, to date, focused exclusively on building alliances between the U.S. and like-minded allies, a group that traditionally excludes emerging countries, in multistakeholder standards development organizations (SDOs). Not considering emerging countries or multilateral SDOs is a strategic mistake. The International Telecommunications Union Telecommunication Standardization Sector (ITU-T), a multilateral SDO, is key for technology governance in emerging countries. To support this view, this study finds that emerging countries participate in standardization efforts at the ITU-T in coalitions with developed countries to shape future technology governance through technical standards, but more often with China and Russia than with the U.S. and its allies. The U.S. and its allies should consider the ITU-T as a key forum for technology competition and participate proactively with emerging countries to shape the future of technology governance.

KEYWORDS: Emerging countries, coalitions, U.S.-China, technical standards, technology governance, International Telecommunications Union, geopolitics

1 INTRODUCTION

To date, the role of emerging countries in multilateral standards development organizations (SDOs) such as the ITU-T has been overlooked by the U.S. and its allies. Limited studies have been conducted to understand emerging countries' participation in the ITU-T as well as in wider standardization activities.[1] In multilateral SDOs, where decisions are made by "one country, one vote," the activities and objectives of emerging countries are consequential. This study will provide a broad overview of which emerging countries have shaped technical standards

1 See Tugendhat & Voo (2021) for some initial research exploring African countries' support for China's New IP proposal. See also Sharp & Kolkman (2020).

at the ITU-T between 2017 and 2021 (the most recent ITU-T study period). This analysis differs from existing studies of geopolitics, technology governance, and technical standards at the ITU-T because it does not focus solely on China and its threat to the West (Hoffman et al., 2020, p. 26), but instead seeks to understand emerging countries and their objectives and behaviors independently. A fresh perspective on the dynamics at the ITU-T will allow us not only to better understand emerging countries' roles in shaping digital technologies but also to identify possible areas of mutual interest for the U.S. to shape emerging technologies in SDOs with new groups of allies, including both traditional, like-minded allies and emerging countries.

Drawing on written contributions from emerging countries at the ITU-T between 2017 and 2021, this study will explore the following questions:

1. Which emerging countries have tried to shape technical standards at the ITU-T?
2. What areas of technical standardization have they been most active in?
3. Who in the ITU-T have emerging countries built coalitions with to shape technology governance?

2 WHAT ARE TECHNICAL STANDARDS AND HOW ARE THEY RELEVANT FOR GEOPOLITICS?

International technical standards are key to technology governance and central to global trade, technology competition, and, increasingly, geopolitics. Technical standards enable the reader to access this paper from a desktop, MacBook, tablet, or Android device. They are central to interoperability and connectivity. Examples of well-known technical standards are USB, Wi-Fi, and 4/5G.

Technical standards are voluntary product specifications that can be developed by a variety of actors but are predominantly developed by industry. International technical standards are negotiated in various SDOs, and the approach governments take toward influencing international technical standards varies from country to country, where on one end of the spectrum some countries take a more hands-off, industry-led approach (e.g., the U.S.) and on the other end, countries have a more centralized approach (e.g., China).

However, while many standards appear to be neutral, benign, merely technical, obscure, and removed from daily life, they are, as argued by Busch (2011, p. 28), an unrecognized but extremely important and growing source of social, political, and economic relations of power. As elaborated by Ruhlig (2021, pp. 4–7), technical standards infer power in a variety of dimensions, including economic, legal, political, and discursive. First, in terms of economic power, a large number of technical standards include patented technology, where licensing schemes are used to protect inventions and promote interoperability and safety. Patents essential for complying with a technical standard are described as Standard Essential Patents (SEPs), which transfer significant royalty fees to the inventors of the innovative technologies. For example, Ericsson earned €5.2 billion in 2017 from SEPs, accounting for 20% of company revenues. As reported in 2021, up to February 1, 2021, Huawei topped the leaderboard with more than 15% of all 5G patents (IPanalytics, 2021). There is, also, a cost for companies who must alter the design of their products or services to comply with standards of a certain market to ensure interoperability. Second, from a legal perspective, although technical standards are voluntary technical specifications, they can become legally binding, where 98% of international trade is affected by the WTO ("About WRO," n.d.). Third, politically, standards can create geographically bifurcated technological zones because certain standards are applied in some regions and alternative standards in others. Standards create lock-in effects and path dependencies, and it is then costly and difficult to replace a whole ecosystem with alternative standards after the fact. On a related note, this dependency on a certain standard that may be dominated by a specific company can introduce a security dimension where, for example, providers of critical infrastructure would have an element of additional control. This is particularly the case with digital technologies, where cybersecurity vulnerabilities could be a significant national security concern. For example, the path

dependency of 5G worries the U.S. and European countries because of the economic and geopolitical advantage it would bestow. Fourth, technical standards influence the discursive dimension, where how technology is designed is political; it inscribes ethical values to it and, when broadly adopted, shapes what is perceived by users as normal. Technical standards that could affect algorithmic bias, transparency in algorithmic decision-making, and privacy are examples of influence over discursive dimensions.

How technology is designed is political; it inscribes ethical values to it and, when broadly adopted, shapes what is perceived by users as normal.

International technical standards have broad and far-reaching implications. The international proliferation of technology is driven through two main routes: (1) from below, through product adoption at such a high volume that a de facto standard is set, or (2) from above, through proposing and securing agreement for technical standards in SDOs and thereby setting a de jure standard (Voo, 2019).

3 STANDARDS MAKERS & STANDARDS TAKERS: DEVELOPED & EMERGING COUNTRIES

Influencing technical standards is traditionally the remit of developed countries, with emerging countries adopting the standards set by developed countries. In these cases, developed countries are the standards makers and emerging countries the standards takers. Developed countries have both made the investment in the research and development to produce the leading technologies as well as housed the companies that disseminate these technologies. National standards adopted at the international level help to proliferate a certain type of technology globally. Emerging countries are often not at the forefront of technology and therefore become standards takers, buying their technology from developed countries.

Indeed, in most multistakeholder SDOs, the key players are the world's most influential technology companies, research institutes, and technical experts. These organizations and individuals disproportionately tend to be from or have been educated in the West or, increasingly, China. China's increased participation and influence over technology and its differing vision of how technology should be governed has captured the attention of governments from Washington to Brussels. Chinese delegations are now among the largest participating in SDOs (Hoffman et al., 2020), and it is reported that Chinese companies work together in lockstep; even ostensible competitors will set aside differences to support another Chinese business.[2] In recent years this has resulted in a flurry of political commitments and national strategies from the U.S. and its allies to respond to the challenge of an increasingly influential China in technology governance (StandICT.eu 2023, 2022).

However, this exclusive focus on China to the exclusion of other countries involved in international standardization efforts is limiting. China's efforts to introduce a new internet protocol at the ITU-T is merely a symptom of a longer-term effort to influence technologies that Beijing and its allies seek to influence. While it is positive that the case of New IP, China's effort to introduce a technical standard to replace the current internet protocols, kick-started an effort by the U.S., Europe, and the UK to coordinate more comprehensively on international standardization efforts

2 Lenovo initially expressed preference for one type of 5G standard LDPC at 3GPP, in opposition to Huawei's Polar Codes. Lenovo Chairman Liu later retracted the company's support for LDC in line with Huawei, as described by Levy (2020).

for emerging technologies, the current approach will not secure U.S. and allied visions for technology governance in the long term, because it excludes the majority of the world in which digital ecosystems are yet to be built.

Many—including the U.S. and its allies—argue that the most influential SDOs are multistakeholder organizations led by industry or technical experts, rather than multilateral SDOs such as the ITU-T. As stated by the G7 in 2021, "we have committed to stronger international cooperation within the G7 and with like-minded partners to support industry-led, inclusive, multistakeholder approaches for the development of digital technical standards in line with our core values" (G7, 2021, p. 1). The statement goes on to obliquely critique China's centralized approach to technology governance and organizations such as the ITU-T, stating that "we firmly state our opposition to any government-imposed approaches that fundamentally seek to reshape the digital technical standards ecosystem" (G7, 2021, p. 1). There is a clear preference for the U.S. and its allies to support standardization efforts in multistakeholder, not multilateral, SDOs.

Accessing technical standardization is hard for emerging countries,[3] but due to the unique nature of the ITU-T, its UN mandate, and the decisive role that governments have within it, it is a "gateway to standardization" for emerging countries. International standardization at the ITU-T is technology diplomacy. National governments pursue their interests and horse-trade in the sidelines. In a "one country, one vote" organization, winning over emerging countries—most of the countries in the world—becomes a strategic imperative. Much work at the ITU-T is conducted by region, and member states (MS) often operate in blocs. For example, the African bloc is 54 countries; thus, winning the support of the African bloc grants an MS 54 votes in support of its interests.

Emerging countries do have agency. These countries recognize their power as both providers of the critical support developed countries need to "win" to pursue their interests in the ITU-T, and also as markets for developed countries and their industries. International standards can codify what types of technologies are to be adopted in certain areas, and these codifications outline which companies meet the requirements. A huge amount of money lurks behind the scenes of technical standards debates, and emerging countries utilize their leverage accordingly.

Disregarding emerging countries or ignoring the influence of the ITU-T are significant mistakes. As elsewhere in the UN, the U.S. and its allies make up only a minority of democratic governments. The ITU-T should not be disregarded as a less consequential forum for technical standardization. The fact that a significant majority of other countries around the world want to use the ITU-T as a forum to standardize emerging technologies makes the activities of the forum consequential and should therefore be prioritized as a forum to take seriously, invest in, and engage proactively with.

4 WHAT IS THE INTERNATIONAL TELECOMMUNICATIONS UNION AND THE ITU-T?

The International Telecommunications Union is one of the oldest United Nations organizations. It was founded in 1865 as a specialized agency for information and communication technologies. Their objective is to "facilitate interconnectivity in communication networks … allocate global radio spectrum and satellite orbits, develop the technical standards that ensure networks and technologies seamlessly interconnect, and strive to improve access to information and communication technologies (ICTs) to underserved communities worldwide" ("About ITU," 2022). The ITU's work is split into three sectors: the ITU-Radiocommunication Sector (ITU-R), which oversees global radio spectrum and satellite orbits; the ITU-Telecommunication Standardization Sector (ITU-T), which develops technical standards, referred to as Recommendations within the ITU; and the ITU-Telecommunication Development Sector (ITU-D), which works to improve access to ICTs ("What Does the ITU Do?," 2022). The focus of this paper is solely on the activities of ITU-T.

3 Interview conducted on May 6, 2022.

The ITU-T is an example of a multilateral SDO, where each country gets one vote, and that country's national committee coordinates its position for a given standards proposal among various stakeholders from that country. Multistakeholder SDOs, on the other hand, may adopt a variety of different structures. In some organizations companies can vote, and in others each expert gets their own vote. Due to the limited role of industry in the ITU-T, one of the chief criticisms is that the standards developed there will not be relevant.

ITU-T's work is divided into study periods. One study period, typically four years long, has a defined set of work items through which the development of Recommendations—or technical standards for ICTs—is pursued. As shown in Table 1, during the most recent completed study period (2017–2021) there were 11 study groups that guided the standardization activities of member states (MS). MS submit written contributions to make proposals, comment on other contributions, and express support or opposition to standardization activities.

TABLE 1. ITU-T Study Groups, 2017–2021

STUDY GROUP	TITLE
2	Operational Aspects
3	Economic & Policy Issues
5	Environment, EMF, & Circular Economy
9	Broadband, Cable & TV
11	Protocols, Testing, & Combating Counterfeiting
12	Performance, QoS, & QoE
13	Future Networks
15	Transport, Access, & Home
16	Multimedia & Digital Technologies
17	Security
20	Internet of Things (IoT), Smart Cities, & Communities

5 METHODOLOGY

The data for this research has been drawn from written contributions made by MS in ITU-T study groups during the 2017–2021 study period. The data has been classified into country contributions; for example, a contribution made by a ministry of a country is attributed to that country. If a contribution is made by an industry representative, then the contribution is assigned to the country in which that company's headquarters is located. If the contribution was submitted by a consortium, i.e., two or more contributing countries, then it has no country assigned to it. This dataset is augmented by interviews with ITU-T participants and relevant stakeholders.

6 OVERVIEW OF FINDINGS

During the 2017–2021 study period, ITU-T member countries submitted a total of 10,435 contributions across 11 study groups. The 10,435 contributions came from a mix of individual countries, consortia of two countries or more, and regional and international organizations.

6.1 INDIVIDUAL COUNTRY CONTRIBUTIONS

Emerging countries submitted 7.6% of total contributions during that period. Seventy-eight emerging countries submitted contributions either individually or as part of a consortium to shape technical standards activities at the ITU-T across all 11 study groups.

TABLE 2. Emerging Countries That Submitted Individual Member Contributions, 2017-2021

AMERICAS (9)	ASIA PACIFIC (8)	EUROPE & CENTRAL ASIA (2)	MIDDLE EAST & NORTH AFRICA (12)	SUB-SAHARAN AFRICA (32)
Argentina	Bangladesh	Kazakhstan	Afghanistan	Benin
Brazil	India	Serbia	Algeria	Botswana
Colombia	Laos		Bahrain	Burkina Faso
Costa Rica	Malaysia		Egypt	Burundi
Ecuador	Nepal		Iran	Cameroon
Haiti	Papua New Guinea		Jordan	Cape Verde
Honduras	Sri Lanka		Oman	Central African Republic
Mexico	Vietnam		Palestine	Chad
Venezuela			Saudi Arabia	Comoros
			Syria	Congo
			Tunisia	Côte d'Ivoire
			Yemen	Democratic Republic of Congo
				Eswatini
				Gambia
				Ghana
				Guinea
				Kenya
				Liberia
				Madagascar
				Mali
				Mauritania
				Mozambique
				Niger
				Nigeria
				Rwanda
				Senegal
				Sierra Leone
				Sudan
				Togo
				Uganda
				Zambia
				Zimbabwe

Between 2017 and 2021, 63 emerging countries submitted individual contributions at ITU-T.

The average number of contributions per emerging country is 12, but the range was significant (1–99). There were only 21 countries that contributed more than 12 contributions each. These were, in descending order, Brazil, India, Democratic Republic of Congo, Egypt, Argentina, Central African Republic, Benin, Sudan, Uganda, Ghana, Guinea, Cameroon, Senegal, Gambia, Iran, Rwanda, Tunisia, Nigeria, Comoros, Bangladesh, and Mali.

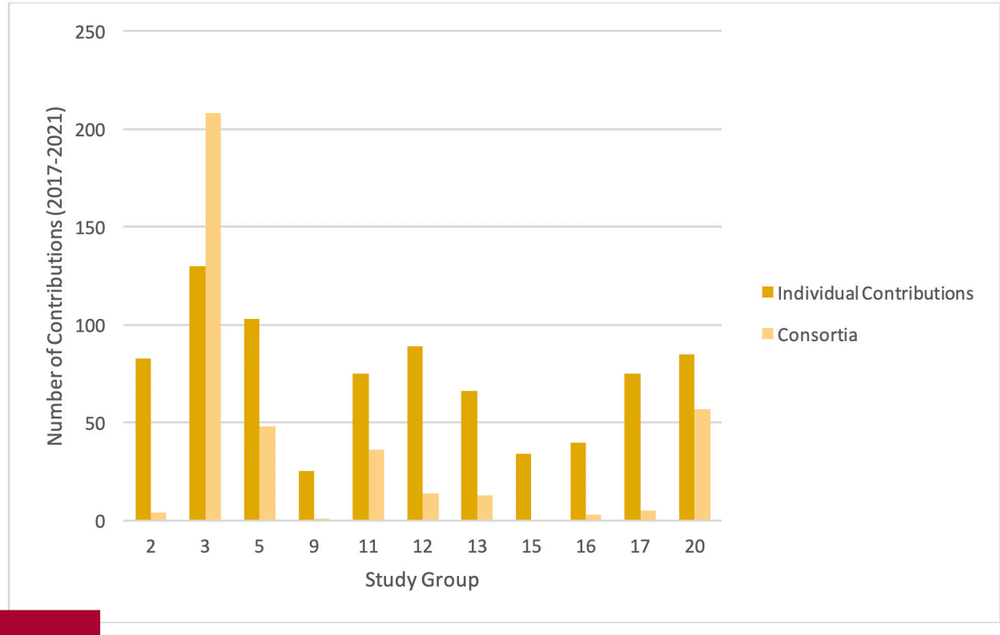
6.2 CONSORTIA

Emerging countries also shaped technical standards through consortia, with nearly 400 contributions garnering emerging countries' written support. It is notable that 24

TABLE 3. Emerging Countries Named on Consortium Contributions Only, 2017–2021

AMERICAS (9)	ASIA PACIFIC (1)	EUROPE & CENTRAL ASIA (5)	MIDDLE EAST & NORTH AFRICA (2)	SUB-SAHARAN AFRICA (7)
Bahamas	Bhutan	Armenia	Kuwait	Lesotho
Cuba		Azerbaijan	Lebanon	Malawi
Dominican Republic		Belarus		São Tomé and Príncipe
El Salvador		Kyrgyzstan		Somalia
Haiti		Uzbekistan		South Sudan
Nicaragua				Swaziland
Paraguay				Tanzania
Trinidad and Tobago				
Uruguay				

FIGURE 1. Emerging Countries' Individual and Consortia Contributions Across Study Groups



emerging countries did not submit individual contributions, submitting only as part of a consortium.

Figure 1 shows that emerging countries were most active in Study Groups 3 (Economic and Policy Issues), 5 (Environment, EMF, and Circular Economy) and 20, (IoT, Smart Cities, and Communities). The study groups in which emerging countries were least active were Study Group 9 (Broadband, Cable, and TV), 15 (Transport, Access, and Home), and 16 (Multimedia and Digital Technologies).

Patterns of behavior and engagement differed across study groups. Individual contributions by MS were the main mode of interaction at the ITU-T, although it is notable that it was not the dominant mode of engagement in Study Group 3.

6.3 STUDY GROUP 20: Internet of Things and Smart Cities

While the majority of consortium contributions from emerging countries were made by a group consisting only of emerging countries, there were 54 contributions made by consortia of emerging countries and Russia, 32 contributions made by consortia of emerging countries and China (and some other developed countries), and 27 contributions made by consortia of emerging countries and the Republic of Korea. Consortia that involved the U.S. or European countries did not surpass a handful each, and the U.S. was part of only one consortium that included an emerging country. It is notable that all of Russia's consortia included only Central Asia/former Soviet States. In contrast, consortia involving China and the Republic of Korea included emerging countries from outside of the Asia Pacific region.

In Study Group 20, emerging countries submitted contributions on a wide range of subjects, including those that were specific to their developing status, geography, and politics; were in partnership with developed economies; and were sometimes in support of the agenda of developed economies. Several submissions focused on bridging the technical divide of countries, e.g., in Africa. There were submissions that advocated for the ITU-T to produce standards for IoT that would drive greater fiber-optic coverage across Africa, as well as broader standards for basic infrastructure for smart cities and communities to stimulate the digital economy. Developing economies also made contributions that were specific to their political realities; for example, the "Draft Recommendations for Smart Demilitarized Zones" proposed a continent-wide solution for smart border monitoring in hotspot regions of Africa to eliminate the need for standing armies and to identify who started border conflicts. Other developing countries have submitted contributions in partnership with developed countries, including on standards for agriculture, sustainability, and AI for IoT. Finally, a couple of contributions in Study Group 20 appeared to involve developing countries in Central Asia signing on in support of Russia's proposal to use Digital Object Architecture[4] as a system for verifying IoT.

7 CONCLUSION

This paper shows that emerging countries are participating in international standardization efforts at the ITU-T, a fact that is not reflected in existing studies on geopolitics and technical standards. While emerging country participation in international standardization efforts at the ITU-T is limited in comparison to developed countries—the original standards makers—emerging countries' needs should be considered more deeply when discussing the future of technology ecosystems, particularly on the part of certain developed Western countries.

This initial study shows that there are three areas wherein emerging countries notably participate in ITU-T activities. Of these, only one is pure standardization: IoT. When emerging countries participate in coalitions, they overwhelmingly form them with Russia, China, and the Republic of Korea.

4 Digital Object Architecture (DOA) is primarily a document repository mechanism used by libraries, e.g., the Library of Congress or the British Library. DOA identifiers are assigned to books, papers, etc., and stored in a searchable database. DOA is a technical framework that some parties believe could be applied to assign unique identifiers to products such as IoT devices, allowing identification, use, and control. The risks are that DOA can facilitate real-time surveillance and tracking of devices and individuals connected to the internet. Russia and Saudi Arabia are seeking to ensure that DOA is adopted as a global standard. This centralization would be a particular risk to human rights defenders and certain minority groups. It could also be equally useful for governments seeking to defend against botnet attacks. See Wiley Connect (2016).

The regional spread of the consortia suggests that China has a greater global reach than Russia, with South Korea not too far behind. It is not clear whether this tendency is because the U.S. and its allies have failed to win emerging countries over, but it is apparent that an opportunity for coalition building has been underutilized or even overlooked. Emerging countries are more aligned with the major competitors of the U.S. and its allies, which suggests that, at least at the national government level, the current trajectory for the future of the digital ecosystem in emerging countries is likely to be more aligned with China and Russia than with the U.S. and its allies.

8 RECOMMENDATIONS

This paper provides five recommendations to further enhance our understanding of emerging countries' participation in standardization efforts and to reduce the risk of the U.S. and its allies failing to build coalitions with a broad set of like-minded countries to pursue shared interests in international standards for digital technologies.

1. *Recognize the value of the ITU-T standardization sector and participate proactively.*

Recognize that the participation of a majority of emerging countries in standardization activities in the ITU-T makes this SDO consequential as a key forum for influencing the future of technology governance in the yet-to-be built digital ecosystems on the other side of the digital divide. The U.S. and its allies should broaden its coalitions to include partnerships with emerging countries.

2. *Develop a detailed understanding of what technologies and international standards are needed or being used in emerging economies and work with allies to provide alternative solutions.*

More analysis is needed to understand why emerging countries have aligned with other developed countries and the benefit gained by both sides through the partnership. These findings should be combined with an analysis of areas of mutual interest in technical standardization efforts among emerging countries, the U.S., and its allies.

3. *Map these international standards back to the standards development organizations in which they originated.*

Identify where the U.S. and its allies could work together to shape standards not only from below but also from above. Further studies need to be conducted to understand to what extent ITU-T Recommendations are adopted into emerging countries' requirements for technology products, particularly around foundational infrastructure.

4. *Align wider policies to complement U.S. standards strategy, e.g., development financing.*

The U.S. government and its allies should align their standards strategies with the development financing for emerging countries. For example, the U.S. government should align the infrastructure projects funded by the U.S. Development Finance Corporation in Africa and Latin America. This alignment will simultaneously help U.S. industry and allies compete for contracts in developing markets and support uptake of preferred technologies, thereby embedding preferred technical standards. Introducing more competition to developing countries would also likely improve the quality of the technology being offered.

The standards development organization ecosystem is broken, with overlapping mandates and deep inefficiencies.

5. *Reform the international SDO ecosystem to be streamlined and inclusive.*

The standards development organization ecosystem is broken, with overlapping mandates and deep inefficiencies. For example, standardization efforts require a significant investment from participants in terms of time and resources, and the process can take multiple years from proposal to an agreed-upon international standard. Even without the threat of geopolitical competition from China, one could see multiple ways to improve international standardization for the good of emerging technologies that are evolving quickly. There is a risk that if a broader effort is not made to improve the system, then it will fail to be fit for purpose. .

a. Streamline the SDO ecosystem. SDOs themselves have varying levels of credibility within the ICT sector. This lack of clarity and efficiency in the system should be remedied so that participants can target their activities more efficiently. Addressing these systemic issues will help stakeholders participate more effectively in SDOs to create quality technical standards. An evidence-based assessment to find the most effective SDOs needs to be done.
b. Make multistakeholder governance truly multistakeholder. Multistakeholder SDOs are not monolithic, and unfortunately many multistakeholder SDOs unwittingly exclude emerging economies and civil society through invisible thresholds, such as the unpaid nature of participation and the high levels of technical expertise required to participate in discussions.

REFERENCES

About ITU (n.d.). International Telecommunications Union. Retrieved May 7, 2022, from https://www.itu.int/en/about/Pages/default.aspx https://www.itu.int:443/en/about/Pages/default.aspx

About WTO. (n.d.). World Trade Organization. Retrieved February 7, 2023, from https://www.wto.org/english/thewto_e/thewto_e.htm

Busch, L. (2011). *Standards: Recipes for Reality.* (2011) MIT Press.

G7. (2021). *G7 Digital and Technology Track - Annex 1: Framework for G7 Collaboration on Digital Technical Standards*. http://www.g8.utoronto.ca/ict/2021-Annex_1__Framework_for_G7_collaboration_on_Digital_Technical_Standards.pdf

Hoffman, S., Lazanski, D., & Taylor, E. (2020, August 29). Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet. *Journal of Cyber Policy, 5*(2). 239–64.

IPanalytics. (2021, February 17). *Who is leading the 5G patent race? A patent landscape analysis on declared SEPs and standards contributions.* IAM. https://www.iam-media.com/article/who-leading-the-5g-patent-race-patent-landscape-analysis-declared-seps-and-standards-contributions

Levy, S. (2020, November 16). Huawei, 5G and the Man Who Conquered Noise. *Wired.* https://www.wired.com/story/huawei-5g-polar-codes-data-breakthrough/

Ruhlig, T. (2021, January). China, Europe and the New Power Competition Over Technical Standards. *Swedish Institute of International Affairs*, 4-7.

Sharp, H. & Kolkman, O. (2020, April 24). *Discussion Paper: An Analysis of the "New IP" Proposal to the ITU-T.* Internet Society. https://www.internetsociety.org/resources/doc/2020/discussion-paper-an-analysis-of-the-new-ip-proposal-to-the-itu-t/

StandICT.eu 2023. (2022, February 9). *An EU Strategy on Standardisation - Setting global standards in support of a resilient, green and digital EU single market*. https://www.standict.eu/eu-standardisation-strategy-2022

Tugendhat, H. & Voo, J. (2021, August). China's Digital Silk Road in Africa and the Future of Internet Governance. *China Africa Research Initiative: Working Papers* (50), 26.

Voo, J. (2019, December). State Influence and Technical Standards. *Harvard Kennedy School Review*. https://ksr.hkspublications.org/2019/12/31/state-influence-and-technical-standards/

"What Does the ITU Do?" (n.d.).International Telecommunications Union. Retrieved May 7, 2022 from https://www.itu.int:443/en/about/Pages/whatwedo.aspx

Wiley Connect. (2016, September 20). *ITU IoT Standards: Gateway to Government Control*. https://www.wileyconnect.com/itu-iot-standards-gateway-to-government-control

Technology, Democracy, and Development

Does the Provision of Digital Technologies Improve the Lives of Rural Communities in Indonesia or Create New Problems?

Subekti Priyadharma

ABSTRACT:

Despite Indonesia's membership in the G20 and its strong economic performance, development in Indonesia is still uneven. Since 1998, the country has adopted a policy of decentralization to strengthen the regions outside Jakarta and Java. However, decentralization still has not addressed the problem of development and economic inequality. Conflicts of interest between the center and the peripheries, and between local governments and their citizens, hinder the development process. President Joko Widodo tried to overcome this problem by issuing a policy of "building from the periphery," which includes the development of digital technology infrastructure to overcome the digital divide. The government's top-down policies are accompanied by bottom-up initiatives from the village development movement, which encourages the active role of the community, and NGOs that bridge the interests of the beneficiaries of development programs and the interests of the government. The tripartite development initiative stakeholders—the government, the community, and NGOs—involve a tripartite contestation of power. The balance, or imbalance, of power between each could result in unintended consequences and impacts. New problems often arise from the presence of external parties or programs, or even the technology itself that is undesired or unanticipated by the local community. The disruptive nature of digital technology often causes a shock to the existing rural social system. This paper illustrates a transformative action research approach that examines two aspects: the unanticipated impacts of digital development, and how the three stakeholder groups respond to these impacts in the form of policy designs and practical solutions.

KEYWORDS: Tripartite development, digital transformation, rural development, center-periphery, decentralization

1 INTRODUCTION

As one of the largest democracies in the world and the biggest emerging economy in Southeast Asia, Indonesia has been with the G20 since its inception in 1999. In December 2021, Indonesia took over the G20 presidency. In 2022, under the motto "Recover Together, Recover Stronger" in relation to the COVID-19 pandemic, President Joko Widodo (known as Jokowi) gave directions that Indonesia will carry out three priority issues at that year's G20 meetings: global health architecture, digital transformation, and sustainable energy transition (The Ministry of Foreign Affairs of the Republic of Indonesia, n.d.).

The government, through the Ministry of Finance, has stated its commitment to allocate a budget of 414 trillion IDR (almost 29 billion USD) or 15% of the 2021 total national budget, for infrastructure building, including digital infrastructure. An extra 30 trillion IDR (more than 2 billion USD) has been added to accelerate digital transformation and strengthen digital connectivity for the post-COVID-19 economy recovery (BPMI Setpres, 2020). The Ministry of Communication and Information has also demonstrated its role in the development of digital technology in rural areas, with programs such as broadband villages and internet villages to support the World Summit of the Information Society (WSIS) agreement concerning providing internet services in rural areas.

The above policies are in line with the priority to pursue digital transformation. To achieve this goal, several working groups have been formed, one of which is the Digital Economic Working Group (DEWG), which discusses three main issues: post-Covid recovery and connectivity, digital literacy and digital talent/skills, and cross-border data flow/data free flow with trust.

The Ministry of Communication and Information, as the supervisor of DEWG, pays special attention to the problem of the digital divide in connectivity issues with a focus on five subtopics, known as the Bali Package: people-centered digital connectivity, digital security as a key enabler to support business continuity, the G20 Digital Innovation Network, the Digital Transformation Expo, and the International Telecommunication Union's (ITU) Smart Village and Smart Island Initiative (The Ministry of Communications and Information of the Republic of Indonesia, 2022). However, there are no clear guidelines on how the government wants to achieve those objectives.

The principles of inclusiveness, empowerment, and sustainability are held in the provision of digital technology so that the 3T regions (*tertinggal, terdepan, terluar*)—the underdeveloped, frontier, and outermost areas in Indonesia located far from the provincial capital—and rural areas are prioritized. This policy follows Jokowi's development principle to "build from the periphery," which he proclaimed in the beginning of his tenure as president in his first term in 2014.

To address this gap, two elements of society, namely nongovernment organizations (NGOs) and civil society movements or organizations (CSOs), have also responded by designing their own programs from the bottom up. They operate in this niche market to serve the interests of rural communities so that they are interconnected. It is not uncommon for the government to ask organizations such as Common Room (CR) and *Gerakan Desa Membangun* (GDM), or Village Development Movement, for their input to assist in formulating national and regional development policies, because they are considered closer to the community and know the field better.

According to UNDP (2006, p. 3), "[t]he term civil society organization (CSO) … encompasses a wider variety of organizations engaged in development work. CSOs comprise the full range of formal and informal organizations within civil society …" including NGOs and community-based organizations (CBOs). Further, Asian Development Bank also includes social movements as one of the categories of CSOs (ADB, 2009). In this paper, CR is categorized as an NGO because it—taken from the definition prepared by ADB (2009, p. 3)—"refers more narrowly to professional, intermediary, and nonprofit organizations that provide or advocate the provision of services relating to" rural internet.

Meanwhile, GDM is not a permanent institution. As the name "Village Development Movement" suggests, GDM is a social movement consisting of networks of villages fighting for common causes. Hence, it is not an NGO but rather one of many forms of CSOs, which is an "informal grouping … of individuals or organizations attempt[ing] to effect social change through sustained, organized, collective action" (ADB, 2009, p. 4).

As an NGO, CR organizes two strategic activities to support

development of community-based rural internet networks and empower rural communities through the Rural Information and Communications Technology (ICT) Camp and the School of Community Networks (SCNs) as part of the program Supporting Community-led Approaches to Addressing the Digital Divide in Indonesia. The project aims "to contribute to building an enabling ecosystem for the emergence and growth of community networks and other community-based connectivity initiatives in five target countries, using an integrated approach over a three-year period" (APC, 2020) that will end in 2023.

On the CSO side, more than a decade ago, in 2011, local leaders from five villages met in Melung Village, Central Java, to form a rural development movement that later became known as *Gerakan Desa Membangun* (GDM). They see themselves as the protagonists of development for their community in which digital technologies function as the "learning facilities capable of bridging village activists in various regions in Indonesia" (Gedhe Nusantara, 2019; author's translation). They argue that information and communications technology has become "a new hope for villages to make a historical leap… [where] villages start to use websites to mainstream rural issues into the wider public sphere" (Gedhe Nusantara, 2019).

We can see that there are at least three parties who play a role in development programs in Indonesia: the government, NGOs, and CSOs, whether organized or not. Throughout this paper, the tripartite constellation on development issues will be referred to as "tripartite development."

Yahya (1999) uses the term tripartite development to refer to the Growth Triangle Model (GTM) in Southeast Asian countries: economic development that is influenced by regional cooperation between three geographically adjacent countries. However, in the case of India, GTM refers to the cooperation between "the central government, state governments and foreign investors" (p. 115). Meanwhile, the term tripartite development is used by Gustavsen (2000) as a reference to cooperation between business and industry, trade unions, and the government. In a similar fashion, Fashoyin (2004) addresses the same parties when he mentions "tripartite cooperation" in relation to employment relations. Studies that review development from the point of view of the government, NGOs, and civil society are not new (e.g., Nugroho, 2010). However, those that review the relationship between the three simultaneously, especially using the term tripartite development in the context of development studies, have not been found.

There are at least three parties who play a role in development programs in Indonesia: the government, NGOs, and CSOs … [a] "tripartite development."

Contestation of power and interest in tripartite development sometimes creates friction between the three parties. Often unintended consequences and new problems arise from the presence of external parties or programs, or even the technology itself that is not desired nor anticipated by the local community. The disruptive nature of digital technology often causes a shock to the existing rural social system, which is culturally structured and entrenched. The friction then raises the question of whether the provision of digital technologies in rural communities in which the projects take place may or may not solve the initial problems or even create new problems for them. This paper examines two aspects, i.e., these unanticipated consequences of tripartite development, both positive and negative, and how the three stakeholder groups respond to these impacts in the form of policy designs and practical solutions.

In Section 2, this paper explains the study's methodology,

and in Section 3 it describes tripartite development in Indonesian rural areas by illustrating development programs led by the government, followed by NGOs, and finally by civil society.

In Section 4, the paper analyzes how digital technology-based development programs initiated by these three parties on the one hand solve development problems related to digital telecommunication infrastructure, but on the other hand create new problems. The paper identifies that in the process of Indonesian rural digitalization, five hurdles need to be overcome: issues of (1) internet access and connectivity, (2) human resource capabilities, (3) aspects of locality, (4) ownership of digital technology, and (5) agency or key actors in development. Following this analysis is a discussion of theories about center-periphery relations, especially from Galtung (1971), and also about development, such as top-down and bottom-up development approaches, and how those theories come into play in digital development in rural communities.

Finally, this paper closes by using the five main issues above to provide five policy recommendations that should be considered as part of mitigating the needs of rural communities for the achievement of rural digital transformation objectives. This can be done by encouraging the synergy of goals, interests, and needs of the tripartite development parties. Mitigation is needed so that digital technology becomes a solution to existing problems, instead of creating new ones.

2 METHODOLOGY

The framework used in this paper is the center-periphery perspective, which allows us to see the balance, or imbalance, of power between those who have the power to make strategic decisions on the formulation and implementation of development programs and those who do not. "Center" can mean the government that has political authority and holds the budget, or NGOs that are supported by donor agencies and have international networks as well as accumulated knowledge resulting from these networks.

NGOs also can be positioned between the inner- and outer-periphery, because they often become intermediaries between the government and society (cf. Habermas, 1996; Priyadharma, 2021). Meanwhile, peripheries can mean rural communities that are geographically, politically, and socially placed in a more inferior position compared to urban communities and the central government, so that they feel the need to carry out resistance both symbolically and technically, as has been done by GDM.

Galtung (1971) explains that in an imperialist system, the center tends to maintain the isolation of its periphery from one another so as to form a feudal center-periphery structure. This paper analyzes how digital communication technology can unlock the periphery's isolation in terms of communication, and also raises concerns about its interaction with the center.

To review development matters, first, this paper takes Sen's (1999) point of view that sees development as a "freedom" with capabilities approach. Second, this paper reviews the dynamics of the top-down development approach applied by the government with the aim of achieving macro development goals in the context of modernization, such as increasing the digital economy and the availability of infrastructure and access to digital technology. These dynamics are challenged by the bottom-up development approach preferred by the rural communities, which is considered more reasonable for responding to local challenges, for example, in the form of mobile application development for public service at the village level.

From the outset, the interplay between these two approaches seems to be contradictory, but we will see how NGOs, which in this case act as intermediaries, play their role in bridging these two interests to achieve more sustainable development goals. Unfortunately, this study did not collect data about the efforts made by the private sector in the digital transformation process, so it cannot reveal the extent to which these efforts are effective or ineffective.

This paper is written based on field research on studies about GDM and CR. While the study of GDM has been completed and published (Priyadharma, 2021), the study of CR with its

School of Community Networks (SCN) is ongoing and has just completed a data collection phase from four locations out of nine target provinces. Transformative action research is deployed especially in the study of SCN, with the aim to contribute to the development of the SCN curriculum (Toomey, 1997; Malcolm et al., 2009; Ramsden & Integrated Primary Health Services Model Research Team, 2003).

3 TRIPARTITE DEVELOPMENT IN INDONESIAN RURAL AREAS

3.1 GOVERNMENT-LED DEVELOPMENT PROGRAMS

Jokowi's development principles are different conceptually from the development paradigm of the two earliest, centralized regimes. Sukarno, as the leader of the Old Order, emphasized political development, while Suharto in the New Order prioritized economic development as a modernization project during his leadership.

The reform era shows a tendency to decentralize political and economic development, which was initiated in 2004 and was marked by the passing of a series of laws on regional autonomy covering governance and regional finance (Law No. 32 and 33/2004 and Law No. 23/2014). The Village Law No. 6/2014 complements the decentralization program because it gives village communities greater authority to manage their resources and plan their own development programs that are more meaningful to their communities.

The Jokowi administration's decentralization program reached its peak when he—in the midst of the debate—signed Law No. 3/2022, which will relocate the state capital from Jakarta to a new area called Nusantara on the eastern part of the island of Borneo. The decision to reposition the center is a severe blow to the perspective of Indonesia's development in the previous regimes, which have been too Jakarta- and Java-centric, resulting in a cavernous development gap with areas outside Java (and Bali).

Inequality in telecommunications infrastructure can be seen from the map of the cellular data networks in Indonesia. Although Indonesia completed the Palapa Ring project, a national fiber optic cable network construction project built with USO funds, in 2019, cellular service providers are still concentrating their business on the island of Java (nPerf, 2022). This is not surprising considering that almost 60% of Indonesia's population lives in Java, even though this island is the smallest among the five main islands.

The Palapa Ring "sky highway" has succeeded in connecting 90 regencies/cities throughout Indonesia and connecting the 3T areas with internet (The Ministry of Communications and Information of the Republic of Indonesia, 2020). The government's efforts to connect villages to the internet and telecommunications networks are manifested in various programs such as Broadband Village, Ringing Village, and Smart Village, as well as previous programs such as District Internet Service Centers (PLIK) and its mobile form (MPLIK), which are currently stalled due to mismanagement.

Even though the government's top-down efforts to connect all regions in Indonesia with the internet network have been massive, there are still too many blank spots not covered by the sky highway. These areas are especially located in villages that are economically unfavorable for internet service providers (ISPs) to do business there, because of the small population number or internet users, low purchasing power, or topography that makes it difficult to build telecommunication infrastructure according to accepted standards.

The above economic problem is not exceptional because it has happened in the past in the offerings of, for example, electricity and post office products in developing countries. This problem is addressed in various ways, such as by (1) using village electrification projects as a political tool to gain votes in disguise of development and maintaining the status quo of the Suharto authoritarian regime (Mohsin, 2014), or (2) offering parallel financial products, such as postal savings and cash-merchants used for remittance service providers and government payments in the development of post office networks in developing countries (Anson et al., 2013).

Even though the government's top-down efforts to connect all regions in Indonesia with the internet network have been massive, there are still too many blank spots not covered by the sky highway.

3.2 NGO AS FACILITATOR AND INTERMEDIARY IN RURAL INTERNET DEVELOPMENT

In order to fill the blank spots left by government programs, Common Room (CR) implements its projects. In 2022, the Rural ICT Camp entered its third year after previously being held twice in *Kasepuhan* Ciptagelar, an indigenous community in the hinterland of the Halimun Salak forest, West Java.

Rural ICT Camp is a series of seminar/webinar activities and online/offline workshops and discussions, where participants share knowledge and best practices, as well as training and exhibitions related to community-based internet infrastructure development in rural and remote places in Indonesia. Participants came from all provinces in Indonesia, with a total number of 682 participants in 2020. The large number of participants was possible because most of them took part in online activity sessions to prevent the transmission of COVID-19.

Government elements from the Ministry of Villages, Development of Disadvantaged Regions and Transmigration, the Ministry of Communication and Information, and the Ministry of Education and Culture support the implementation of Rural ICT Camps by sending representatives to give talks. Other organizations such as ICT Watch, ICT Volunteers, and the Indonesia Association of Internet Service Providers (APJII) back up the event as well.

Carrying the theme "Desa Bangkit, Nusa Bangkit" (the village rises, the nation rises), Rural ICT Camp 2021 highlighted the issue of rural-urban digital divide, which in 2019 was 1:2, where 36% of rural adults, compared to 62% of urban adults, were connected to the internet (The World Bank, 2021). Although internet penetration in Indonesia in 2021 reached 73.7% (Kemp, 2021), which shows rapid growth, 49% of Indonesian adults are still not connected to the internet (The World Bank, 2021). The World Bank estimates that, as of 2020, 43% of Indonesians live in rural areas (The World Bank, 2018). This could be a factor for this inequality, along with the development gap between Java-Bali and the outer regions; the income gap; and gender, education, and generational divides (The World Bank, 2021).

Rural ICT Camp is "expected to shed the light for the rural revival movement as a locus of environmental and cultural-based innovation supported by the utilization of the internet and digital platforms" (Common Room Networks Foundation, 2021a, p. 2). The activities were also prepared as a means for the birth of the School of Community Networks (SCN), where representatives from nine provinces, namely Aceh, West Kalimantan, West Java, West Sulawesi, Lombok, Bali, East Nusa Tenggara, Maluku, and Papua, were invited to attend and participate. The prototypes of the development of community-based internet networks are planned to be located in these provinces.

According to the Association for Progressive Communication (APC), an organization that supports CR, such a project "will catalyze more affordable and inclusive connectivity for underserved or excluded communities in low-income rural, urban and peri-urban areas" (APC, 2020). To achieve its mission, CR promotes the 5L principles deemed appropriate in rural conditions: low tech, low energy, low maintenance, low learning curve, and local support (Belli, 2020). SCN is "part of a strategy to support, develop, and consolidate

citizen initiatives so that they can build an independent and sustainable community-based internet infrastructure in their area" (Common Room Networks Foundation, 2021b, p. 2).

At the time of writing this paper, CR has carried out three Schools of Community Networks (SCNs) activities, in Polewali Mandar Regency (West Sulawesi), Tembok Village (Bali), and Jayapura Regency (Papua), which resulted in three different implementation models. The adoption of SCN is always adapted to the characteristics of the local community. As befits the pluralistic Indonesian society in terms of culture and needs, the prototype produced from the implementation of SCN shows the development of internet networks with various patterns.

From March 20 to 22, 2022, Campalagian District, Polewali Mandar Regency, hosted the first SCN that was initially attended by five villages. They consequently signed a Memorandum of Understanding with CR. However, due to high interest, three other villages from three different districts joined. Each village sent three representatives, most of whom were youths from diverse backgrounds with a fairly balanced composition of men and women. For three days, they were trained by CR trainers and local ICT volunteers on three topics: server management, broadband-based simple internet network construction, and service/content management. The chiefs of those villages are trying to build cooperation that would lead to the formation of the Inter-Village Coordinating Board (BKAD). The board is intended to manage internet services for rural communities in the form of joint village-owned enterprises (BUMDESMA).

A different pattern was found in Tembok Village, Bali, where only one village is involved in the development of internet infrastructure. As in Polewali Mandar, the village chief plays a central role in making decisions in Tembok so that this initiative can continue. Together with ICT volunteers and their village-owned enterprise (BUMDES), and supervised by CR, the community develops a "Super App," which they named "Djangkep,"[1] to facilitate village public services.

In Papua … the participants learned to build a satellite-based internet network … because the broadband internet network (wireless or fiber optics) has not been evenly developed in Papua due to its difficult topography.

The Super App will record community waste bank savings,[2] which can be converted into easy financing for school children's transportation, village health services, health insurance, and other public services. This application also records other population data and speeds up administrative matters and correspondence services needed by village residents digitally, so that people who work outside the area do not need to return to the village to take care of various kinds of certificates.

In contrast, the central role of the village chief was not found in Papua. There, the agent of change is the Agency of Communications and Information, Jayapura Regency, through its head, who is the actor behind various kinds of projects based on digital telecommunication services in the region. The head of the agency has actively assisted in the formation of Pemantik (Pace Mace Admin TIK),[3] a volunteer organization at the forefront of the region's development of internet networks, and the use of ICT for development (ICT4D). Pemantik is ratified through a Regent's Decree and is structurally responsible to the head of the Agency of Communications and Information.

In Papua, the SCN was held from April 20 to 21, 2022, and was attended by 15 participants from Pemantik, staff from the Agency of Communications and Information, and ICT volunteers, which organizationally has a national scope. Unlike what was done in the previous SCNs, here the participants learned to build a satellite-based internet network (VSAT). This was done because the broadband internet network (wireless or fiber optics) has not been evenly developed in Papua due to its difficult topography (full of highlands, mountains, and vast forest areas). Therefore, satellite-based internet service is a reasonable option for those living in remote areas. Building the participants' knowledge and skills to develop a satellite-based internet connection is urgently needed in Papua to help people in remote areas gain internet access.

The implementation of SCN in two other locations, Breuh Island (Aceh) and Ciracap (West Java), did not go according to plan, which led to the postponement of the event for different reasons. In Aceh, the local volunteers have a different vision from CR. While CR wanted the internet network to be built as a community internet prototype, the local organizer demanded an internet infrastructure with a high standard that requires stratospheric costs. In addition, the local team was not able to fulfill the deliveries requested by CR within the agreed deadline.

In Ciracap, the local volunteer unilaterally abandoned the internet service that had been built together with CR at a local vocational high school (SMK). The responsible person did not build a system for managing internet service sustainability. CR received no reports regarding the operation of internet services there, so it decided to restart the collaboration with the SMK by forming a new team. Furthermore, there are no village heads or heads of an agency who take responsibility for organizing and making decisions regarding the development of the internet network, so activities in this area are not sustained. The project failures in Aceh and Ciracap show the misalignment of goals and interests between CR and the local people.

An interesting story of the development of community-based internet networks can be drawn from the indigenous community Ciptagelar, who hosted the Rural ICT Camps twice, in 2020 and 2021. The community has succeeded in independently providing broadband internet services for its residents by collaborating with an ISP, Awinet. This collaboration allows Ciptagelar Hotspot to act as a reseller of internet access to community members with various voucher systems (hourly, daily, weekly, monthly) at small costs (the cheapest is 2000 IDR, or 15 cents USD, for an hour connection).

The key to success in Ciptagelar is not one or several village chiefs nor an office head with a high position and formal government authority, but a traditional leader who is highly respected and obeyed by not only local residents but also residents outside Ciptagelar: Abah Ugi, a visionary and progressive leader. Though he is a traditional leader, he is not anti-technology, especially digital technology. Instead, he encourages progress and change in his area through the use of digital platforms, as long as it does not change customary practices, especially those related to rice farming.

The Ciptagelar indigenous community follows the philosophy of rice as the source of life. Consequently, the rice agriculture tradition cannot be changed from generation

1 "Djangkep" originates from the Balinese language, which means complete, assembled, or plenary. This philosophy reflects Djangkep's goals as an application that offers complete public services, becomes the bridge between rural residents and the village authority, and realizes village good governance (fast, easy, responsive, and adaptive to the needs of the people).

2 The villagers are encouraged to sort and collect household waste and deliver them to a waste collection site. An employee will then weigh the waste and convert it into bank savings that can be withdrawn in cash. Currently, this activity uses another application specifically designed for recording each customer's waste bank savings.

3 "Pace" and "Mace" are greetings for men and women, respectively, in the Papuan language, whereas TIK corresponds to ICT.

to generation, as the community believes this will change or ruin their lives. While no modern technology should be utilized in rice farming, it may be used for other things at Ciptagelar as long as it does not reduce tradition. They refer to this as the principle of *"ditambah boleh, dikurangi jangan"* or "adding but not reducing." This means that people may add tools or technology to support their lives (as long as it is not related to rice farming), but not to reduce tradition. These principles and traditions are properly guarded by Abah Ugi and obeyed by all his citizens.

3.3 GRASSROOTS MOVEMENT AS LOCAL INITIATIVE IN BUILDING RURAL NETWORKS

GDM treats digital technologies as amplifiers of their grassroots movement that seeks to manage village resources and good governance, while criticizing the government's top-down development approach. To achieve this, they initiated *Desa Bersuara*, or the "voicing village"—a strategy for mainstreaming rural issues through village websites with a village-specific domain, "desa.id."

The choice for desa.id (*desa* literally means village in the Indonesian language) is political. The village community does not want to use the "go.id" domain provided by the local government because it would violate the central government's rule that states that a village is not part of the government organizational structure (see the Minister of Communication and Information Regulation No. 28/2006). In addition, the go.id domain does not represent village identity nor respect rural bottom-up initiatives. The village website is also part of the development of the village information system whose provisions are regulated in the Village Law.

Politically, GDM contributed to the implementation of deliberative democracy to oversee the formulation and discussion of the Village Bill before it was passed in 2014. ICT was used to (1) publish session activities via video streaming; (2) organize events to watch parliament sessions in villages together; and (3) build two-way communication between the parliament and the rural community through social media. They named this program Parliament 2.0 (Gedhe Nusantara, 2019).

This action is a deradicalized form of resistance from rural communities on the periphery of power by using digital technology to demolish the information and communication hegemony of the government/parliament at the center, whose activities related to public affairs are not always accessible to the public. Parliament 2.0 shows that mobilization no longer needs to be done physically to put pressure on the center—it is enough to open up digital access to communication and information. GDM claimed that Parliament 2.0 received quite a positive response from various parties, making it easier to raise public opinion to smooth the ratification of the Village Bill.

4 RURAL INTERNET: Solving Problems or Creating New Problems?

This section discusses how the availability of digital technologies can have a positive and negative impact on the lives of rural people. Digital technology will be a solution to problems at the local level if there is alignment of goals and interests of the three parties involved in development. In contrast, new problems will arise if there is a gap in the goals and interests of the three parties. Therefore, we need to see what these parties aim for from the provision of rural digital technologies.

At least five issues should be highlighted in which we observe a clash between development goals and needs at the central and regional levels. This does not mean that other needs, such as digital literacy, cybersecurity, and cross-border data flows, are not addressed by the CR programs, but there are other organizations, namely ICT Watch and ELSAM, who are collaborating with government institutions to tackle those issues (ID-CSO DTTF, 2022).

CR presented the five issues in the civil society's position paper for Indonesia's digital transformation for the 2022 G20 meeting. Table 1 presents an overview of the five main issues in the places where community-based internet projects are located. However, due to space limitation and because some subjects are already elaborated elsewhere (Priyadharma, 2021), not all details are discussed in this paper; instead, only the significant ones are highlighted.

TABLE 1. List of community-based internet projects based on locations and the five main issues

NO.	LOCATION	THE FIVE MAIN ISSUES					IMPACT
		CONNECTIVITY	HR CAPACITY	LOCALITY	OWNERSHIP	AGENCY	
1.	Ciptagelar	Cheap and easy internet access	Regular supervision of internet development by CR trainers	Local TV and radio broadcasting using closed internet circuit	Village cooperation with ISP	Indigenous leader & ICT volunteers	Meaningful vs. universal access: broadband internet service for the community
2.	Polewali Mandar	Intervillage cooperation for simple internet connectivity	Regular training for young people about internet	Local content of village website and social media	Planned intervillage-owned enterprise	Cooperation of village chiefs & ICT volunteers	MoU of intervillage coopera-tion for the program's sustainability
3.	Tembok Village, Bali	"Super App": public service application	Regular supervision of app development by CR trainers	Context-specific data (bottom-up data supply) vs. ODI's general data	Data and app ownership	Village chief & ICT volunteers	Meaningful vs. universal access: the development of Super App Multidata of the village vs. One Data policy of the central and regional government
4.	Jayapura Regency, Papua	Satellite-based internet	Regular training for young people about satellite-based internet	-	Local government and training center in cooperation with ISP	Head of Commu-nication Agency & ICT volunteers (Pemantik)	Meaningful vs. universal access: Internet connection for people in remote areas
5.	Ciracap	-	-	-	-	Lack of leadership/ different goals	Project failure: No alignment of goals and interest
6.	Breuh Island, Aceh	-	-	-	-	Lack of leadership/ different goals	Project failure: No alignment of goals and interest

NO.	LOCATION	THE FIVE MAIN ISSUES					IMPACT
		CONNECTIVITY	HR CAPACITY	LOCALITY	OWNERSHIP	AGENCY	
7.	Melung Village, Banyumas	Village intranetwork (elaborated in Priyadharma, 2021)	Asymmetrical and changing value of knowledge	Village website domain desa.id	Village website domain desa.id	Village chief & rural movement in abolishing the feudal and asymmetrical center-periphery structure	Degradation of traditional knowledge Clash with local government who prefers go.id domain
							Clash with local government who prefers go.id domain

The first issue is *connectivity.* The government's policy to ensure that all rural areas in Indonesia have internet access is a commitment that needs to be appreciated. This commitment is in line with the agreement of the World Summit on the Information Society in 2003 "to connect villages with ICTs and establish community access points" (WSIS, 2003) by 2015 as part of a massive digitalization project to improve connectivity and access, which has not been successfully fulfilled so far.

Many government projects to ensure universal access have left telecommunications infrastructure unproductive. The USO-funded PLIK and MPLIK project was terminated due to corruption allegations and mismanagement after the government established no less than 5,956 PLIK, 1,857 MPLIK, and another 1,222 PLIK in productive centers by December 2013 (The Ministry of Communications and Information of the Republic of Indonesia, 2013). Now, MPLIK vehicles are piled up, rusty, and not functioning; they've become an asset abandoned in vain. In some areas, such as in Polewali Mandar, the vehicle is used as a means of transportation for ICT volunteers to carry out their activities, but it is no longer in accordance with its function as a mobile internet service provider.

This same philosophy is followed in other universal access projects for rural areas such as Broadband Village, Ringing Village (referring to the provision of telephone access), and Smart Village (an upgrade to the Ringing Village by assuring villages have quality internet access by 2025) (ITU, n.d.). The government may claim to have built thousands of access points in all rural areas across the country, but new problems arise about how to manage and sustain the network so that it will not burden village finances and resources. Therefore, in addition to ensuring the provision of hardware and software, the government needs to pay attention to the availability of qualified brainware to utilize the technology.

The universal access policy is a classic development problem rooted in the modernization development paradigm, where the "one-size-fits-all" policy is considered a solution to development problems at the local level, which in this case involves connectivity issues. The government implements a top-down policy (e.g., Ringing Village, etc.) in which rural communities are expected to adopt digital technology provided by the center in the hope of boosting their economic activity.

While the villagers admit that internet is a technology that can bring "light" to the community (previously, "light"[4] was associated with the provision of electricity), universal access alone is not enough. CR recommends the government issue a policy on meaningful access to internet connectivity: contextualized connectivity with local conditions, so that it can be a solution to specific problems and address the needs of the rural community.

Some examples of meaningful access are the focus of Tembok Village on application development of the Super App, the Ciptagelar indigenous community on cheap and easy internet services, Campalagian District (Polewali Mandar) on intervillage cooperation to develop BUMDESMA, and the Regency of Jayapura (Papua) on the development of satellite-based internet infrastructure. Each of these initiatives cannot be replicated in other regions due to the different problems and availability of resources in each, but they still follow the 5L principles. Therefore, instead of replication, community-based internet network development programs suggest "multiplicity" (Servaes, 1999; Servaes & Lie, 2013), which encourages the emergence of more diverse and contextual connectivity models in each region.

An internet network development program is not a "packaged intervention" (Toyama, 2015) that can be duplicated like a policy package implemented in different locations. Instead, from various best practices, other regions can learn to develop meaningful connectivity models for their own communities. This spirit is in accordance with the philosophy of Sen (1999) in *Development as Freedom*, which defines development as "a process of expanding the real freedom that people enjoy" (p. 3). Village communities need freedom and space to realize their development ideas so that they can get recognition for their existence.

The second issue raised by CR is the need to improve the *quality, capability, and skills of human resources* to increase the brainware that will manage the access points built from various projects. The government and elements of civil society need to collaborate and, together with the community, conduct training, workshops, and discussions to increase their knowledge and skills capacity about digital technology relevant to their community. Since 2021, the government has carried out a number of initiatives such as Siberkreasi, a national digital literacy program. However, most of these programs do not specifically target rural residents and, in the midst of the COVID-19 pandemic, are still carried out virtually in the form of webinars.

It is true that the internet opens access to new information and knowledge. Thus, digital communication technology can solve the problem of information impasse and is expected to support the growth of the information- and knowledge-based economy. This is why Kofi Annan, former Secretary General of the United Nations, once encouraged developing countries to take advantage of ICTs so that they have "the chance to leapfrog some of the long and painful stages of development that other countries had to go through" (CNET, 2006). However, we need to be aware that "the advantages and disadvantages of new technologies are never distributed evenly among the population" (Postman, 1998, p. 2) and that the adoption of new technologies by society can result in groups of "winners" and "losers" (Postman, 1998, p. 3).

In the case of the GDM initiative in Melung, a village official, who is also an Imam at the village mosque and a teacher at a recitation school for village children at his home, may suddenly feel "stupid" and "slow" when confronted with new technologies. Digital technology indirectly produces unintended consequences for community groups who are actually the centers in a specific type of knowledge (in this case, religious knowledge), but with no warning are pushed to the periphery and the "loser" group in knowledge about new technologies in the digital age. Unaware, the respective village official degrades his own knowledge, which he has mastered for years, and instantly feels useless in this new era. In other words, there is an "asymmetrical and changing value of knowledge" between one set of knowledge and another (Priyadharma, 2021). That is certainly a new

4 Villagers' statement during field research.

problem undesirably created by the arrival of new (digital) technologies. By increasing the human resource capability in interacting with digital technology, such a problem can be tackled.

The third and fourth issues in the context of rural connectivity relate to the *locality* and *ownership* aspects of the technology provided, especially in its compatibility with national and local regulations. For example, when rural communities develop village information systems independently to collect population data through an app, such as the Super App in Tembok Village, and use it as the basis for village decision-making, this often clashes with the One Data Indonesia (ODI) policy from the central government.

Based on Presidential Regulation No. 39/2019 concerning ODI, data governance policy was issued with the aim "to create quality, accessible and shareable data between central and regional agencies" (The Ministry of National Development Planning, 2021). ODI, through its portal data.go.id, which can be compared with the U.S. Government's open data policy at data.gov, adheres to the principles of transparency and accountability for government data and other public agencies to support national development.

For the purpose of rural development, local communities need to be given the freedom to use context-specific data that they collect themselves from the bottom up, using whatever platforms they develop and own.

From the government's point of view, ODI is conclusive in supporting the planning, implementation, evaluation, and control of development. The ODI system is expected to provide a single and integrated database, supporting government decision-making based on quality data. Previously, government data were scattered in different agencies and ministries, which often displayed asynchronously. The data integration problem was acknowledged in the OGI (Open Government Indonesia) webinar Talk #4 on October 26, 2020, which revealed thousands of independent applications and the sectoral ego of each agency not willing to share their data (OGI National Secretariat, 2020). ODI attempts to solve that problem.

However, ODI's data collection mechanism is still too general and does not specifically address regional needs, especially in rural areas. For example, the search results on data.go.id do not provide a list of relevant answers when searching with the keywords "Desa Tembok," "Ciptagelar," or "Campalagian," which are where SCNs/Rural ICT Camps were held. This is why ODI should not be forced on a top-down basis to become the only database for designing development programs in an area and for measuring its performance. On the contrary, for the purpose of rural development, local communities need to be given the freedom to use context-specific data that they collect themselves from the bottom up, using whatever platforms they develop and own.

During the focus group discussion conducted in Tembok Village on March 31, 2022, it was revealed that the Super App, developed without the involvement of the government, is intended to answer local problems with the village administration system and public services. Nevertheless, representatives from the regency's Agency of Communication and Information reminded the group that the data collected by the Super App should not violate the ODI principles and should be stored on the Agency's server in order to minimize data misuse, guarantee data security, and protect data from "going out." On the one hand, the government's vision of ODI can be understood in supporting national development policies, but on the other hand, ODI can reduce the "aspect of locality" and the "sense of ownership" of the village data.

Another case study on locality and technology ownership is the decision of the villages in the GDM network to use desa.id as their website domain instead of choosing the go.id provided by the government. As has been discussed above, the village feels that the *desa* domain name is more representative of the village community and thus represents their locality. They also have a high sense of ownership of the desa.id domain because it is the result of their long effort debating with many sides to officially formalize the use of the domain (Priyadharma, 2021).

The last issue reveals the *agency* problem, which is crucial for the success of a development program. Two dimensions that need to be emphasized here are the issue of leadership and the relationship between actors at the center and the regions. The balance, or imbalance, of power between center and periphery could result in different outcomes, because both the center and the periphery have different needs, resources, and social capital to meet these needs, as described below.

First, discussion of the previous four main issues revealed that the existence of a leader, both organic (coming from inside the community itself) and inorganic (part of the local government structure or coming from outside the community), is a key factor in the process of rural communities adopting and adapting digital technology. Ciptagelar's indigenous leader Abah Ugi, the chief of Tembok Village, the head of the Communication Agency of the Jayapura Regency, and all of the village chiefs in Polewali Mandar are good examples of local leaders playing their role in the development sector, while one of the reasons for the program failure in Ciracap and Aceh was the lack of effective leadership. In addition, the engagement and crucial role of ICT volunteers in those locations as agents of change mean that the collaboration of leaders and members of civil society is very much needed in supporting the achievement of the program objectives.

We should take note that Indonesia consists of hundreds of various local cultures and customs, which leads to different social capital in each region and different leadership models, so it is very difficult to replicate one model in other places. Therefore, each region, assisted by relevant stakeholders, needs to develop its own digital technology-based development model that is in accordance with the local context and can be studied by other regions.

Second, the internet changes, if not eliminates, the feudal and asymmetrical center-periphery structure as described by Galtung (1971), where "interaction with the outside world is *monopolized* by the center …" (p. 85; emphasis in original). In this context, the center is the government that, especially during the New Order era, depoliticized the villages and made them into a "floating mass" so as to not respond to political issues (Aspinall & Fealy, 2010). With a feudal structure like this, rural communities are prevented from building solidarity and networks with each other, thus maintaining the state's "asymmetrical mechanism of imperialism" (Galtung, 1971). Moreover, we can also look at this case from the perspective of ownership of the village. Who has power over the village? Is it the village community itself in the periphery, or the local ruler in the form of a local government as the center within the periphery (Galtung, 1971)? Who is the agent in such a structure?

Based on the observation in Melung Village, GDM formed a new network-based, center-periphery relationship structure from the communicative use of the internet so that they can interact and build solidarity between fellow rural communities (Priyadharma, 2021). CR aims for the construction of such a structure as well with its SCN project. In addition, direct communication can also be established with the government and parliament at the national level, without the need for a bureaucratic process to go through the regional government at the local level as a direct superior to the village administration.

This is an agency as well as a communication problem between rural communities and the local government. On the one hand, the internet, and especially social media, can solve the problem of communication feudality, i.e., communication inefficiency in government structures where bureaucracy is often an obstacle. On the other hand, tensions arise as the local government feels that their authority is being bypassed or their intermediary functions are ignored in communicating with the central government and the rural

we see a new problem arise—power contestation between the village administration and the local government in terms of bureaucratic communication, so that there are times when village initiatives in developing internet networks are not supported by the local government.

The provisional conclusion that can be drawn from all the case studies described above is that an alignment of goals, interests, and needs of the three parties is required in a rural development program. From all locations, perhaps Jayapura and Polewali Mandar Regency reflect this alignment, because they show a synergistic collaboration between elements of the government (either village administration or local government), NGOs (in this case CR), and CSOs, namely the ICT volunteer group, which in Jayapura is Pemantik. Although the programs in Tembok Village and Ciptagelar indigenous communities can be said to be running quite well, the fact that the involvement of government elements is minimal shows that this alignment has not existed so far. However, this situation is still very likely to change, because the program for the provision of community-based internet in Indonesia and the data collection process of this research are still ongoing. The government, too, is still working on digital transformation projects throughout Indonesia to welcome the G20 Summit in Bali in November 2022.

5 CONCLUSION AND POLICY RECOMMENDATIONS

"[A]ll technological change is a trade-off … Technology giveth and technology taketh away. This means that for every advantage a new technology offers, there is always a corresponding disadvantage" (Postman, 1998, p. 1). That is the first thesis of Neil Postman in his talk *Five Things We Need to Know About Technological Change*. This paper analyzes how the arrival and use of digital technology initiated by the three parties (i.e., government, NGOs, and civil society) in rural communities solved problems or actually created new problems. This section provides policy recommendations, based on the five issues in digital development in rural areas, to address the problems that arise as a result of these issues.

1. *Focus on multiplicity rather than replication for connectivity access and contextual digital technology.*

The provision of universal internet access does not necessarily solve the problem of information and communication at the local level. Therefore, instead of replication, the recommended policy is multiplicity: more meaningful access for the community concerned, so that digital technology is more contextual and differentiated. The government needs to be more supportive of rural initiatives who, together with NGOs, operate in niche markets not touched by established ISPs because, businesswise, they are not profitable enough. Rural communities need certainty and regulatory guarantees to implement development ideas and achieve their life goals. This paper recommends that the government consider issuing a special license for community networks that would make its holder eligible to access separate funds (e.g., Universal Service Funds, or USF) to finance a range of community initiatives, from the building of adaptive internet infrastructure, to local content development, and to the increase of local capability.

2. *Improve human resource capacity and capability while respecting traditional knowledge.*

It is important to improve the quality of brainware, or human resource capacity, of rural communities who will take advantage of the digital technology (software and hardware) being built. Referring to Sen (1999), this "capabilities approach" is needed for people "to lead the kind of lives they value—and have reason to value" (p. 18). This approach is important to note because the increase in HR capabilities is one of the benchmarks for a country's Human Development Index (HDI) score. The improvement of human capabilities for the purpose of their meaningful interaction with digital technologies is key, so that no one is left behind in the world's digital transformation process.

Affirmative policies for vulnerable and marginalized groups need to be taken apart from being in accordance with Jokowi's development principle of "building from the periphery," and to prevent the formation of new "losers" or new problems as a result of the provision of digital technologies in the Indonesian rural communities. Digital literacy programs have to be contextualized to solve local problems, not detached from local values and knowledge, which need to be respected and should not be negatively compared to modern-day knowledge. This will ensure that rural communities who master traditional knowledge are not forced to abandon their value system for the adoption of digital technologies. Instead, these new technologies should help them preserve what they think they have reason to value (Sen, 1999).

3. *Allow for rural community data locality and ownership.*

As the debate over the government's policy of One Data Indonesia (ODI) versus the village's persistence to supply context-specific data from the bottom-up reveals, policies must pay attention to the issue of data/technology locality and its aspect of ownership, which are the third and fourth issues in rural digital development. If rural communities are given the freedom to collect and process their own data, decisions taken at the village level would more accurately tackle local problems. Such policy confirms Sen's "freedom-centered understanding … of the process of development [that] is very much an agent-oriented view" (1999, p. 11).

Furthermore, the internet and algorithms need to be directed to serve the public interest by encouraging the community to feed the platform with relevant information and data for the benefit of the community itself, so that we can have an open, transparent, and accountable platform (see Fuchs & Unterberger, 2021). That way, data supply adheres to a participatory principle, where the community is involved in providing data by "pushing" it from the bottom, and is not just monopolized by the government, where data is "pulled" from above.

4. *Recognize rural communities' agency by engaging local leaders and allowing community-based digital development.*

All stakeholders need to pay attention to the issue of agency. First, individuals must be given the freedom to develop a leadership model that fits the sociocultural conditions in which the development project is implemented. Again, Sen (1999) suggests that individuals "need not to be seen primarily as passive recipients of the benefits of cunning development programs" (p. 11), but as independent and sustainable agents. The government as a policymaker needs to positively recognize the role of local/traditional leaders and engage as well as and manage them, along with the traditional values and rituals that they adhere to, to make digital transformation programs in rural areas sustainable and meaningful.

Individuals must be given the freedom to develop a leadership model that fits the sociocultural conditions in which the development project is implemented.

The second aspect of agency concerns center-periphery relations. To overcome its feudal structure of relations and rural communities' communication "unfreedom" (see Sen, 1999), or lack of communication freedom, this paper recommends that digital telecommunication policies allow communities to develop community-based internet networks legally. Concretely, rural communities need legal support so that they can work with ISPs to become resellers on a local scale with affordable fee schemes. Policymakers should avoid directly prohibiting or even punishing people who try to build internet networks for their own communities, especially if there are no commercial services from ISPs available in that location. Such actions will only demotivate the community and kill community initiatives

that are essential for a growing digital innovation climate.

Additionally, all parties need to acknowledge each other's interest so that each of them does not try to achieve only their own goals, without heeding those of the others. For example, ISPs should not only orient to the size of the market but also provide services to those who live in remote areas. The government should not only seek to complete development projects but also pay attention to whether that type of project is really needed by the local community or whether the project will sustain in the long run. Beneficiaries also need to understand that NGOs and the government are often limited by time and targets for their project deliveries, so that what happened in Aceh and Ciracap, with the suspension of the SCN program, can be avoided.

REFERENCES

ADB. (2009). *Civil Society Organization Sourcebook: A Staff Guide to Cooperation with Civil Society Organizations*. Asian Development Bank.

Anson, J., Berthaud, A., Klapper, L., & Singer, D. (2013). Financial Inclusion and the Role of the Post Office. *World Bank Policy Research Working Paper No. 6630*, Available at SSRN: https://ssrn.com/abstract=2343708.

APC. (2020). *Supporting Community-led Approaches to Addressing the Digital Divide*. Association for Progressive Communications. Retrieved April 26, 2022, from https://www.apc.org/en/project/supporting-community-led-approaches-addressing-digital-divide#:~:text=The%20%E2%80%9CSupporting%20Community%2Dled%20Approaches,over%20a%20three%2Dyear%20period

Aspinall, E., & Fealy, G. (2010). Introduction: Soeharto's New Order and its Legacy. In E. Aspinall & G. Fealy (Eds.), *Soeharto's New Order and its Legacy. Essays in honor of Harold Crouch (Asian Studies Series, 2)*, pp. 1–14. Canberra: ANU E Press.

Belli, L. (Ed.). (2020). *Community-based Internet: A Practical Guideline to Community-Based Internet Infrastructure Development*. Common Room Networks Foundation.

BPMI Setpres. (2020). Belanja Infrastruktur 2021 untuk Penguatan Infrastruktur Digital dan Penunjang Dasar [2021 Infrastructure Spending for Strengthening Digital Infrastructure and Basic Support]. Retrieved May 2, 2022, from https://www.presidenri.go.id/siaran-pers/belanja-infrastruktur-2021-untuk-penguatan-infrastruktur-digital-dan-penunjang-dasar/

CNET. (2006). *Kofi Annan's IT challenge to Silicon Valley*. Retrieved April 30, 2022, from http://www.cnet.com/news/kofi-annans-it-challenge-to-silicon-valley/

Common Room Networks Foundation. (2021a). *Summary Report: Rural ICT Camp 2021* (Unpublished).

Common Room Networks Foundation. (2021b). *Preliminary Study: School of Community Networks Development in Indonesia* [Unpublished].

Fashoyin, T. (2004). Tripartite Cooperation, Social Dialogue and National Development. *International Labour Review, 143*(4), 341–372.

Fuchs, C., & Unterberger, K. (Eds.). (2021). *The Public Service Media and Public Service Internet Manifesto.* University of Westminster Press.

Galtung, J. (1971). A Structural Theory of Imperialism. *Journal of Peace Research, 8*(2), 81–117.

Gedhe Nusantara. (2019). Gerakan Desa Membangun [Village Development Movement]. Retrieved May 3, 2022, from https://www.gedhe.or.id/?s=Gerakan+Desa+Membangun

Gustavsen, B. (2000). A Norwegian Initiative for a Tripartite Development Program. *Concepts and Transformation, 5*(1), 125–131.

Habermas, J. (1996). *Between Facts and Norms. Contributions to a Discourse Theory of Law and Democracy.* MIT Press.

ID-CSO DTTF. (2022). Tiga Tantangan Utama Transformasi Digital Indonesia [Three Main Challenges of Indonesia's Digital Transformation]. *Civil Society's Position Paper for DEWG of G20 Presidency of Indonesia.* Indonesia Civil Society Organization of Digital Transformation Task Force.

ITU. (n.d.). Program I: "Program Desa Berdering (DB) 2010" (Ringing Village Program). Providing Telephone Access to all Villages by 2010. Retrieved April 29, 2022, from http://www.itu.int/net4/wsis/stocktaking/projects/Project/Details?projectId=1142329345

Kemp, S. (2021). *Digital 2021: Indonesia*. DataReportal. Retrieved May 3, 2022, from https://datareportal.com/reports/digital-2021-indonesia

Malcolm, C., Gopal, N., Keane, M., & Kyle, W. C. (2009). Transformative action research: Issues and dilemmas in working with two rural South African communities. *Researching possibilities in mathematics, science and technology education*, 193-212.

Mohsin, A. (2014). Wiring the New Order: Indonesian Village Electrification and Patrimonial Technopolitics (1966–1998). *SOJOURN: Journal of Social Issues in Southeast Asia, 29*(1), 63–95.

nPerf. (2022). *Cellular Data Networks in Indonesia*. Retrieved April 24, 2022, from https://www.nperf.com/en/map/ID/-/-/signal/?ll=-2.5678942164342513&lg=118.01999999999998&zoom=5

Nugroho, Y. (2010). NGOs, the Internet and Sustainable Rural Development. *Information, Communication & Society, 13*(1), 88–120.

OGI National Secretariat. (2020). Peran Satu Data Indonesia dalam Mewujudkan Pemerintahan yang Terbuka [The Role of Satu Data Indonesia to Propel the Practices of Open Government]. *OGI News*. National Secretariat of OGI, The Ministry of National Development Planning. Retrieved April 29, 2022, from http://ogi.bappenas.go.id/storage/files/news/licnnCihtfGkp8SSOQTdRdlo8jZReMOg5bXuEo2o.pdf

Postman, N. (1998). *Five Things We Need to Know About Technological Change*. Retrieved May 4, 2022, from https://web.cs.ucdavis.edu/~rogaway/classes/188/materials/postman.pdf

Priyadharma, S. (2021). *Internet and Social Change in Rural Indonesia: From Development Communication to Communication Development in Decentralized Indonesia.* Springer Nature.

Ramsden, V. R., & Integrated Primary Health Services Model Research Team (2003). Learning with the community. Evolution to transformative action research. *Canadian Family Physician, 49*, 195.

Sen, A. (1999). *Development as Freedom*. Oxford University Press.

Servaes, J. (1999). *Communication of Development: One World, Multiple Cultures*. Hampton Press, Inc.

Servaes, J. & Lie, R. (2013). Sustainable Social Change and Communication. *Communication Research Trends, 32*(4).

The Ministry of Communications and Information of the Republic of Indonesia. (2013). *Siaran Pers Tentang Laporan Akhir Tahun 2013 Kementerian Kominfo [Press Release: 2013 Annual Report of the Ministry of Communications and Information]*. Retrieved April 29, 2022, from https://kominfo.go.id/index.php/content/detail/3702/Siaran+Pers+No.+100-PIH-KOMINFO-12-2013+tentang+Laporan+Akhir+Tahun+2013+Kementerian+Kominfo+/0/siaran_pers

The Ministry of Communications and Information of the Republic of Indonesia. (2020). *Palapa Ring*. Retrieved April 24, 2022, from https://aptika.kominfo.go.id/2020/01/palapa-ring/

The Ministry of Communications and Information of the Republic of Indonesia. (2022). *Susun Bali Package, Menkominfo: Delegasi DEWG Bahas Lima Isu Konektivitas Digital [Arranging Bali Package, The Ministry of Communication and Information: DEWG Delegation Discusses Five Digital Connectivity Issues]*. Retrieved July 1, 2022, from https://www.kominfo.go.id/content/detail/41902/siaran-pers-no-192hmkominfo052022-tentang-susun-bali-package-menkominfo-delegasi-dewg-bahas-lima-isu-konektivitas-digital/0/siaran_pers

The Ministry of Foreign Affairs of the Republic of Indonesia. (n.d.). *Indonesia G20 Presidency 2022*. Retrieved January 17, 2023, from https://kemlu.go.id/madrid/en/pages/presidensi_g20_di_indonesia/5101/etc-menu

The Ministry of National Development Planning. (2021). *Tentang Satu Data Indonesia [About One Data Indonesia]*. Retrieved April 29, 2022, from https://data.go.id/tentang

The World Bank. (2018). *Rural population (% of total population) – Indonesia*. Retrieved June 29, 2022, from https://data.worldbank.org/indicator/SP.RUR.TOTL.ZS?locations=ID

The World Bank. (2021). *Beyond Unicorns: Harnessing Digital Technologies for Inclusion in Indonesia*. https://www.worldbank.org/en/country/indonesia/publication/beyond-unicorns-harnessing-digital-technologies-for-inclusion-in-indonesia

Toomey, R. (1997). Transformative Action Research. *Educational Action Research, 5*(1), 105–121.

Toyama, K. (2015). *Geek Heresy: Rescuing Social Change from the Cult of Technology* (Kindle Edition). Public Affairs.

UNDP. (2006). *UNDP and Civil Society Organizations: A Toolkit for Strengthening Partnerships*. United Nations Development Programme.

WSIS. (2003). *Geneva Plan of Action. Article 6, Point a.* World Summit on the Information Society. Retrieved April 29, 2022, from https://www.itu.int/net/wsis/docs/geneva/official/poa.html

Yahya, F. (1999). *Decentralizing Economic Development in India and the Emergence of Growth Centers* [Doctoral Thesis, University of Sydney]. Retrieved April 30, 2022, from https://ses.library.usyd.edu.au/handle/2123/27693

Conclusion

Technology governance was long left to market forces; in the United States in particular, the prevailing idea was that this would lead to the best outcomes for democracy. After decades of inaction on the part of most democratic governments, technology policy is now a priority for almost every government in the world. Yet this momentum does not necessarily lead to a shared approach, and instead political differences and fragmentation among various governments guide the ideology underpinning regulatory interventions. A fierce competition has broken out around the question of who gets to set rules and standards for technologies and the internet itself. The idea is that the first mover can scale and have a global ripple effect. Authoritarian regimes continue to consider technologies useful instruments for state control and to deploy artificial intelligence (AI) for surveillance and social media platforms for propaganda or censorship. Democratic governments may prioritize antitrust enforcement or civil rights protections in the digital realm. It is a high-stakes battle that must be thoroughly researched and understood to inform public policymaking.

Much of the focus in academic research and the think tank world investigates technology policy as it evolves in Brussels and Washington. Some also look at policymaking around technology in Delhi and Beijing. At Stanford's Cyber Policy Center, the major global powers have dominated our focus, too. With this edited volume we wish to widen our lens to include scholarship of the specific policy developments in emerging countries.

No technology operates in isolation. Technological specificities are powerful and important: facial recognition systems challenge the promise of privacy protection, and automatic weapons alter how we consider the battlefield. But beyond that, the legal, political, economic, and social contexts determine how the use of technologies impacts people. Are there laws in place that protect them? Or does the law primarily protect the state? Between the role of cryptocurrencies in Argentina or the use of chat apps in Iran, not only are the specifics of any given technology decisive for the impact on society, but so is the context in which they are used.

The impact on people, their insights, and the experiences of populations in emerging countries is essential to gauge, not in the least because they often face the consequences of American-made technologies. Decisions made in boardrooms thousands of miles away can become a matter of life and death. Victims of the genocide in Myanmar accuse Facebook and its algorithmic setting of amplifying hate speech, while OpenAI used cheap outsourced labor in Kenya to moderate content of its ChatGPT AI-trained bot. We need the voices of people directly impacted to inform the leaders of technology firms. Too often, an appreciation of the different contexts and the realities of communities in which products and services will be used is missing in Silicon Valley. Social media platforms were enthusiastically hailed as vehicles for individual emancipation and access to information. Yet in the absence of speech and broader legal protections, there may not be freedom after expression, and a network-

ing technology can be used to map networks of activists to round them up and imprison them. Cryptocurrencies were sold as shields against corrupt authorities, but, without laws to oversee them, ended up defrauding gullible people. Similarly, regulatory initiatives in the EU, such as the General Data Protection Regulation (GDPR), have seen bits and pieces ripped out of context and used as pretext for repression elsewhere.

The impact of repressive policies makes studying them particularly challenging. For many, academic freedom is not a guarantee, and seeking access to information on the state's use of surveillance tools can be dangerous. We appreciate that even in our efforts to include a variety of voices in this edited volume, there are many that remain unheard.

Beyond the domestic impact of technology policies, emerging countries play a growing role in shaping international policies. Their politics and alignments, with democratic coalitions or authoritarian ones, will end up shaping multilateral frameworks and agreements that have global reverberations. It is not a given that democratic countries will be able to shape global rules. Investments into infrastructure and dependencies on supply chains are only some of the incentives at play in emerging markets. They support alignment with China and its agenda at the United Nations, for example. Unfortunately, both the impacts on local communities and the chances of a democratic process for standard- and rule-setting can be negatively affected. In many cases, there is no outside influence needed for a government to use international rules to justify a stronger grip at home. A deeper understanding of these dynamics is needed, as well as stronger leadership from democratic governments. Capacity-building and partnering to train and prepare officials for complex negotiations can offer a counterweight. Under any circumstance, the democracies of this world should lead by example. Without a federal data privacy act in the United States, for its government to condemn others rings hollow. Similarly, a condemnation of a foreign state for seeking stealthy access to people's data through technology companies is undermined by the practice of U.S. intelligence services doing exactly that.

When American technology companies lobby against new legislation in Washington, it is often with their own business bottom line in mind. What is overlooked is the fact that laws also ensure checks on governmental behavior and avoid the abuse of power by governments. Unfortunately, democratic governments, too, have used new technologies to strengthen state institutions at the expense of people and their rights. All over the world there are examples of how governments of various political colors have seen new technologies as new tools for control and retention of their own power. That dynamic makes it additionally challenging to push for regulatory change in countries with repressive governments.

We thank the authors for their research and hope they have widened your perspectives on the scope of impact of technology policy worldwide. This volume is the first step toward a more sustainable initiative to foster deeper research into policy questions around emerging technologies in emerging countries. Stanford's Cyber Policy Center has the ambition to continue to be more inclusive of perspectives from communities around the world as we tackle policy lacunae and developments. We look forward to inviting scholars and new partners to join us in this mission.

Marietje Schaake
Stanford University
International Policy Director, Cyber Policy Center
International Policy Fellow, Institute for Human-Centered Artificial Intelligence

Contributing Authors

Cecil Abungu is a visiting researcher at the Centre for the Study of Existential Risk (University of Cambridge), where he primarily works on a book project tracking the place of future generations in indigenous African peoples' thought. He also works with the AI:FAR team on projects touching on how AI could lead to extreme inequality and power concentration. He has a background in law, including as an Open Philanthropy research grantee. He is also a research affiliate at the Legal Priorities Project and coordinator of the ILINA Program. He holds an undergraduate law degree from Strathmore Law School in Nairobi and an LLM from Harvard Law School.

Kimberly Anastácio is an internet governance and critical infrastructure researcher and PhD candidate at the American University School of Communication. She studies the sociopolitical implications of the internet technical structure. Her present research draws on document data and in-depth interviews to understand how organizations that create standards for information and communication technologies care for the environment. Kimberly received a BA and an MA in Political Science from the University of Brasília. She has worked at the Department of Public Policy Analysis of the Getúlio Vargas Foundation, a center for applied social research fostering innovation in public policies. She also has experience with advocacy efforts in the Brazilian National Congress on the human rights implications of the internet.

Bridget Boakye is the Artificial Intelligence (AI) policy lead at the Tony Blair Institute for Global Change. Her work focuses on AI policy and ethics, start-ups and innovation, internet policy, and resetting the global narrative of Africa through tech. Her previous work includes data science and analytics, and business development and strategy.

Adi Guyo is an undergraduate student at Strathmore Law School in Nairobi. During her time in law school, she has served as an editor with the *Strathmore Law Review* and participated in several research projects touching on subjects as diverse as law and technology, space law, and moral philosophy. Later this year, Adi is set to start her master's degree in Public International Law at the Geneva Graduate Institute, where she intends to continue building her research portfolio.

Matías Jackson is a legal consultant for national and international organizations in digital rights, telecommunications regulation, and platform governance. Among others, he has worked for Amnesty International, UNESCO, the University of Columbia, and the Inter-American Dialogue. He is also an internet law lecturer at the University of the Republic of Uruguay and a visiting professor at the Center for Technology and Society of the Fundaçao Getulio Vargas, Rio de Janeiro. He graduated from the University of the Republic Uruguay, where he also obtained a postgraduate diploma in Information Systems and IT Management. He received an LLM in Intellectual

Property with the Highest Honors from George Washington University thanks to a Fulbright Scholarship.

Jhalak M. Kakkar is executive director at the Centre for Communication Governance at the National Law University Delhi, where she is also a visiting professor. At CCG she leads the academic and policy research across information technology law and policy issues. Jhalak serves on the board (Academic Constituency-Alternate Member) of the Global Network Initiative and the Steering Committee for the Action Coalition on Meaningful Transparency. At the Global Partnership on AI, Jhalak is an expert member of the Multistakeholder Experts Group Plenary and is a member of the Working Group on Data Governance. She is an expert member of the UN Broadband Commission Working Group on AI Capacity Building. She is also an expert on the Asian Dialogue on AI Governance. Prior to CCG, she was a visiting researcher at Harvard Law School focused on artificial intelligence governance and fintech and blockchain regulation. She has also served as an editor on the *Harvard Journal for Law and Technology*. Jhalak received her LLM from Harvard Law School on a Fulbright-Nehru Masters Fellowship and holds an integrated social science and law degree from the National University of Juridical Sciences, Kolkata, India.

Andreas Kuehn is a senior fellow at Observer Research Foundation America, where he leads research on international technology policy and cybersecurity. His work focuses on new risks and challenges in international security at the intersection of digital technology, supply chain security, and governance. He currently examines the formation of technology alliances among like-minded, democratic states to manage strategic technology competition, specifically regarding 5G and semiconductors. Prior to joining ORF America, Andreas was a senior program associate at the EastWest Institute, where he worked on U.S.-Russia and U.S.-China cybersecurity issues. Before that, he was a cybersecurity fellow at Stanford University and an adjunct researcher at RAND Corporation. He holds an MSc in Information Systems from the University of Zurich and a PhD in Information Science and Technology from Syracuse University.

Danielle Youlan Luo works at the nexus between geopolitics and financial markets. Her research primarily focuses on global tech governance, how data regulations can support both privacy protection and digital economies, and geopolitical and political risk management. She earned a BA in Political Science and International Relations from the University of British Columbia.

Maia Levy Daniel is a lawyer and tech policy and regulation specialist. She is a research associate at the Center for Studies on Technology and Society (CETyS) in Argentina and public policy advisor at Wikimedia Argentina. Maia was director of research and public policy at Centro Latam Digital in Mexico and has worked with organizations across sectors in the U.S. and Latin America, as well as with international organizations such as UNESCO. She has written extensively around platform governance and regulation, content moderation and speech issues, artificial intelligence governance, and digital rights.

Panthea Pourmalek is a senior research officer at the Global Network of Women Peacebuilders, and a master's student at the School of Public Policy and Global Affairs at the University of British Columbia, Canada. Her research and professional interests lie in gender, peace and security, technology, and global tech governance. She is especially interested in the applications of emerging and cutting-edge technologies to conflict settings, peace processes, and peacebuilding. She has published on global digital governance, the role of ICTs in women-led peacebuilding, technology-facilitated gender-based violence against women peacebuilders, and global digital governance. Her current research explores gender and cybersecurity, and women-led peacebuilding in Armenia, Azerbaijan, and Lebanon.

Subekti Priyadharma is a lecturer at the Faculty of Communication Sciences, Universitas Padjajaran in Bandung, Indonesia. He holds an MA (2008) and earned his PhD (2021) in media and communication science from the University of Erfurt, Germany. He received a DAAD (German Academic Exchange Service) scholarship for his doctorate. His dissertation, "Internet and Social Change in Rural Indonesia: From Development Communication to Communication Development in Decentralized Indonesia,"

was published by Springer Nature in 2021. Subekti is working as a researcher for Common Room Networks Foundation within the program "Connecting the Unconnected: Supporting Community-led Approaches to Addressing the Digital Divide." The program includes policy and regulation research for community networks in Indonesia, which is supported by the Association for Progressive Communications (APC). Subekti has a versatile teaching and research profile, such as digital communication technology and society, communication and social change, and fundamentals of communication science, especially qualitative social research. He recently began a position as a visiting lecturer and research associate at the University of Erfurt and teaches, among others, qualitative research methods, Information and Communication Technology for Development (ICT4D), and Southeast Asian media systems.

Trisha Ray is a fellow and deputy director at the Centre for Security, Strategy and Technology at the Observer Research Foundation in India. Her research focuses on geopolitical and security trends in relation to emerging technologies, including AI, 5G, and semiconductors. She also chairs ORF's annual tech conference, CyFy. Trisha is a member of UNESCO's Information Accessibility Working Group, a Pacific Forum Young Leader, as well as a 2022 Schmidt Futures International Strategy Forum Fellow. Prior to her current post, Trisha was a program assistant at the Asia Society Policy Institute in Washington, DC, where she researched and wrote on national AI strategies in Asia, nuclear issues, and India-US security relations. She also helped convene forums to engage U.S. lawmakers, academics, and embassy officials on U.S. trade, technology, and security policy for Asia. Trisha completed an MA in Security Studies from the Walsh School of Foreign Service at Georgetown University, and a BA (Honors) in Journalism from Lady Shri Ram College, Delhi University.

Mariana Sanchez Santos is a PhD candidate in the School of Communication at American University. She holds a BA in International Relations from ITAM in Mexico City and an MA in Political Communication from the University of Leeds, UK. She has also taken courses at City University of Hong Kong, Universidad de San Andrés in Buenos Aires, Stanford University, and Oxford University. Her doctoral research focuses on political communication, elections, and technology in Mexico. Prior to joining American University, she worked for different offices of the government of Mexico, as a consultant to media companies, and as a communications officer to the Fulbright Program in Mexico. She also worked as a research assistant in the Civil Society and Philanthropy Project from ITAM.

Inga Kristina Trauthig is the head of research of the Propaganda Research Lab at the Center for Media Engagement at The University of Texas at Austin. Previously, she has been a research fellow with the International Centre for the Study of Radicalisation at the Department of War Studies at King's College, London. She received a PhD from King's College, London, and an MLitt from the University of St. Andrews in Middle Eastern, Caucasus, and Central Asian Security Studies. She is interested in understanding violent and nonviolent extremism, the manipulation of political competition, and other societal impacts of emerging technologies. Over the last few years, she has mainly focused on the Middle East and North Africa, particularly Libya. She is also an associate with the Institute of Middle Eastern Studies at King's College, London, the Konrad Adenauer Foundation or Candid Foundation in Berlin. Previous positions include an associate fellowship at Al Sharq Forum Istanbul, a visiting researcher position at George Washington University in Washington, DC, and the United States Institute of Peace in Tunisia. Her work has been featured by outlets like *Al Jazeera, BBC, CNN, Houston Chronicle, Foreign Policy*, and *The Washington Post.*

Julia Voo is a cyber fellow at Harvard's Belfer Center, where she leads the team behind the National Cyber Power Index, and the director of Cyber and Tech Policy at HP Inc. She was formerly the research director for the China Cyber Policy Initiative. Her other areas of research concern geopolitics and technical standards geotech and the Digital Silk Road. A 2019 graduate of Harvard Kennedy School's Master's in Public Administration program, Julia served earlier at the British Embassy in Beijing, where she covered China's cyber and AI policy from a commercial perspective, technical standards, and other trade policy issues. She lived in Beijing

for seven years with stints at the EU Delegation to China and the Carnegie-Tsinghua Centre for Global Policy, and she has spent time at the UK's Cabinet Office. Julia's research, writings, and commentary have featured in several media outlets, including the *Financial Times*, the *Economist*, BBC World News, *Wired Magazine*, and Cyberscoop.

Editors

Marietje Schaake is the international policy director at the Stanford University Cyber Policy Center and international policy fellow at Stanford's Institute for Human-Centered Artificial Intelligence. Between 2009 and 2019, Marietje served as a Member of European Parliament for the Dutch liberal democratic party, where she focused on trade, foreign affairs, and technology policies. Marietje is an (advisory) board member with a number of nonprofits including MERICS, ECFR, ORF, and AccessNow. She writes a monthly column for the *Financial Times* and a biweekly column for the Dutch *NRC* newspaper.

Francis Fukuyama is the Olivier Nomellini Senior Fellow at Stanford University's Freeman Spogli Institute for International Studies (FSI), and a faculty member of FSI's Center on Democracy, Development, and the Rule of Law. He is also director of Stanford's Master's in International Policy Program, and a professor (by courtesy) of Political Science.

Acknowledgements

The editors of this volume would like to thank a number of people who assisted in the preparation of this volume. It was done under the auspices of the Program on Democracy and the Internet, part of the Cyber Policy Center at Stanford University's Freeman Spogli Institute for International Studies, and the Stanford Program on Philanthropy and Civil Society. Their directors, Nate Persily and Rob Reich, gave us valuable support. Haifa Badi Uz Zaman, Alessandro Vecchiato, and Ben Rosenthal played critical roles in the organization of this project. We are also grateful to Eden Beck for her work in editing the volume and Johanna Friedman for her work in designing the volume.

Marietje Schaake
Francis Fukuyama

Stanford | Cyber Policy Center
Freeman Spogli Institute and Stanford Law School