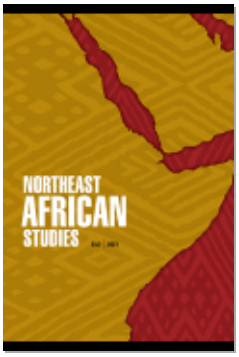
PROJECT MUSE

Contested Space and Self-Determination: The Dynamics of Ethiopia's Digital Space



Kebene Wodajo

Northeast African Studies, Volume 21, Number 2, 2021, pp. 227-264
(Article)

Published by Michigan State University Press

For additional information about this article
https://muse.jhu.edu/article/866997

[Access provided at 7 Mar 2023 07:29 GMT from Universitat St. Gallen]

SPECIAL ISSUE

Contested Space and Self-Determination: The Dynamics of Ethiopia's Digital Space

Kebene Wodajo
University of St. Gallen

ABSTRACT

Government-to-people and people-to-people relationships are increasingly mediated and configured by emerging technologies, necessitating new ways of framing and understanding the role of government and digital technologies in the social order. Recent sociopolitical developments in Ethiopia demonstrate how digital platforms have become a space for contested narratives and a division of interests between socioeconomic policies and political views. By addressing the major technologically assisted counterpower movements in Ethiopia between 2015 and 2021, this article examines digitally mediated encounters and configurations that are struggling to produce a specific form of subjectivity. The article examines digitally mediated encounters and the patterns of the relationships among main actors in the digital space—users, the government, and platform technologies—through the lens of the network theory of power. The article problematizes the deployment of state surveillance, rulemaking and regulatory leverages, and the gatekeeping role of platform technologies

Kebene Wodajo, "Contested Space and Self-Determination: The Dynamics of Ethiopia's Digital Space," *Northeast African Studies*, Vol. 21, No. 2, 2021, pp. 227–264. ISSN 0740-9133. © 2021 The Author(s). All rights reserved.

in modulating and suppressing the emergence of a self-determined critical mass. As a remedial approach to addressing the risks inherent in intersecting state–corporate configuration and surveillance, the article proposes a broadly defined yet context-specific right to privacy that enables self-development, protects a socially and culturally constructed emergent self, and encourages the capacity for self-determination. To analyze the right to privacy as a remedy, the study uses a critical legal analysis of privacy rights with a focus on the 1995 Ethiopian Constitution. Throughout the analysis, it seeks to highlight three overarching arguments that have relevance beyond the specific case of Ethiopia. First, it challenges the assumption that the digital space is a neutral and free space. It argues that digital platforms provide venues for contested and rival narratives and interests, and that not every actor in the digital space has equal leverage over the digital infrastructure. The digital space therefore manifests an asymmetric power relationship. Second, it argues that the capacity of citizens for self-development and self-determination is increasingly modulated by expansive surveillance and the regulatory leverage of state and corporate power, which is used to suppress the emergence of critical mass. It therefore argues that third, there is a pressing need for the reinterpretation of legal protection for privacy rights as a protection for a socially and culturally constructed emergent self. By addressing this need, protection will be offered to the capacity for self-determination, critical subjectivity and democracy.

Introduction: Setting the Scene

Ethiopia is a federation of linguistically, culturally, and ethnically diverse people. However, in contrast to its diversity, the country has always been a society with heavy state control on its communication infrastructure, with only one state-owned telecommunication service provider, Ethio Telecom, until recently. Records show that Ethiopia has been among the most digitally repressive states over the past twenty-eight years.[1] The Ethiopian People's Revolutionary Democratic Front (EPRDF), which ruled the country between 1991 and 2018, used its regulatory power over the country's digital and communication infrastructure to moderate what citizens could see and know about political, social, and economic issues. In doing so, it attempted

to create submissive, uncritical, and predictable mass, although with little success.

Despite heavy state media control and digital repression[2], Ethiopian citizens—mostly younger people from the regional states of Oromia and Amhara, and those in the diaspora—used nonmainstream communication means such as social media platforms[3] to challenge state power. They mobilized a series of counterpower mass movements that eventually succeeded in toppling the EPRDF regime in 2018. However, although this process sent the country towards a much hoped for political transition, little has improved in terms of freedom of expression or thought, or privacy rights. This article will examine digitally mediated power and counterpower relationships as a struggle between the emergent critical mass that challenges repressive state power and the tendency of the incumbent government that strives to suppress such emergence by narrowing and sometimes denying the space in which a critical mass could flourish. The increasing deployment and use of new digital and communication technologies facilitates both sides of these relationships, turning digital media into a contested space between those who seek to maximize the power that they hold (although in different form) and those who seek to challenge and redefine that power.

Recent experiences—including but not limited to Occupy Wall Street,[4] the Mexican movement #YoSoy132,[5] the Barcelona *indignadas* movement,[6] the BurmaNet movement,[7] Arab Spring,[8] and #BlackLivesMatter[9] illustrate how the fundamental contradictions within a society translate into a longing for social justice,[10] democracy,[11] and self-determination.[12] The Ethiopian case of digitally mediated counterpower movements fits what Manuel Castells[13] refers to as a power and counterpower, or a domination and counterdomination relationship in a networked society. Ethiopia and its ruling elites have a long history of power and counterpower relationships,[14] but what distinguishes the confrontations between 2015 and 2021 is that platform technologies have significantly mediated the relationship. To address the influence of these technologies, this article focuses on Ethiopia's digitally assisted counterpower movements between 2015 and 2021 as well as the relationship patterns between the main actors in the digital space, namely the state-to-people and people-to-people relationships and the role of digital platforms and the companies that run them in the process.

Between 2015 and 2021, Ethiopian politics witnessed constant power versus counterpower movements protesting against the government in different parts of the country. These movements, although similar in many ways, also had their own peculiarities in terms of demands and narratives, which shaped the pattern of intergroup convergence and divergence (or collaboration and confrontation). The major movements were the Oromo Protests (2015–20), the Sidama People's Movement for Statehood (2019), the Amhara Youth Protest Movement (2016–18), and the #TigraiGenocide campaign against the war in the Tigray region (2020–21). It can be argued that the change in political landscape and ideological narratives that followed the regime change in 2018 significantly reshaped demands, narratives, and forms of power versus counterpower relationships during this period. Thus, for clarity and logical structure, the article divides this period into two main sections—pre-2018 (between 2015 and 2018) and post-2018 (between 2019 and 2021, or the post-EPRDF period).

The period between 2015 and 2018 was marked by resistance, and although there were several actors involved in the counterpower mass movement, the role of the Oromo youth movement in Oromia regional state stands out. The Oromo are an ethnic group that embodies modern Ethiopia and represents the largest contributing state in the federation in terms of both population and size. The Oromo protest was led by the *qubee* generation (*dhaloota qubee*), a youth group from a rural background that was schooled using *qubee*, a written language of the Oromo people, providing its members with college-level education and advanced digital literacy.[15] The immediate trigger for the 2015 Oromo protest was the government's integrated Addis Ababa Master Plan, which sought to expand the capital into the surrounding areas.[16]The Oromo protest movement was later joined by the Amhara youth protest against the identity and administrative policy of the representatives of the Welkait Amhara Identity Committee in 2016. The Amhara are the second-largest ethnic group in Ethiopia after the Oromo, and the two mass movements sparked other anti-government protests across the country, shaking Ethiopia's deep-seated political and economic structure of injustice to the core and bringing down the EPRDF regime—which had ruled the country since 1991—in 2018.

The post-2018 period (between 2019 and 2021) experienced major sociopolitical changes that significantly altered the counterpower demands, participants, and modes of expression. These changes included the gradual exit of the Tigray People's Liberation Front-led/EPRDF (TPLF/EPRDF) from the governing regime and the advent of a transitional regime led by Abiy Ahmed. Following the regime change, political narratives began to shift sympathetically towards the formation of a centralized and unitarized state structure via the restructuring of the existing ethnolingual federation, a process that infuriated pro-federalist groups in the country and increased interethnic tensions. By 2019, the situation had been aggravated by high profile assassinations and the imprisonment of opposition political leaders.[17] Meanwhile, the deterioration of human rights conditions and media freedom culminated in a mismanaged and failed transition to democracy. The situation worsened in 2020 with the outbreak of war in Tigray with devastating humanitarian consequences in the region,[18] and with the infamous election of 2021.[19] The cumulative effect of these sociopolitical crises shifted the power and counterpower movements in terms of demands, participants, and modes of resistance against the government. For instance, counterpower movements gained strength through digital activism, demands were refocused from mere socioeconomic justice to the political right to self-determination. Meanwhile, new areas of resistance by groups such as the people of Tigray, who after remaining passive during the pre-2018 counterpower movements now become active counterpower platform users, especially after the breakout of war in Tigray regional state. At the same time, the anti-government movement in Amhara was calmed and morphed into a position of allegiance with the new government.

Almost all mass movements organized by different groups between 2015 and 2021 took on a hybrid nature that fused virtual and physical spaces. Activism in the virtual space was robustly integrated and fed by defiance on the ground, especially in the case of the pre-2018 Oromo protests. The physical and virtual space intersected to form structures upon which to mobilize efforts, contextualize, and articulate protest demands, and expose and interrogate human rights abuses, exploitation, and rights violations by government and corporate powers.[20] Strategies were devised and information was gathered and communicated predominantly using Facebook (now

Meta[21]), but also through other platforms such as Twitter, Telegram, WhatsApp, and email. Protests and their associated demands were disseminated via social media through status updates, private messages, profile pictures, infographics, videos, and photographs.

Although these hybrid counterpower movements will be used as the main body of this case study, the aim of the article is not to analyze the movements and the repressive political environment of pre- and post-2018 Ethiopia in which they flourished. Instead, by looking at cases of digitally assisted counterpower movements, the article seeks to map relational patterns and encounters in order to identify the nature and purpose of encounters between different actors in the digital space in the process of power versus counterpower to find out what they sought to achieve. In particular, it focuses on the nature of encounters between those who resisted power by using digital platforms, the government—which sought to suppress mass uprisings by deploying its rulemaking and regulatory leverage—and platform-owning companies who acted as gatekeepers of the digital infrastructure.

By using this approach, the article attempts to highlight the major encounters in the power versus counterpower processes, which this article categorizes as horizontal people-to-people encounters, vertical government-to-people encounters, and the configurations made by platform owning companies in this process. The first of these three processes, horizontal encounters, includes digitally mediated people-to-people encounters or relationships in which individuals and groups reconstruct the digital space to create, reveal or expand their stories, narratives, and collective identities as members of a community. The second, vertical government-to-people encounters, represents encounters in which state surveillance and rulemaking powers were used as a means of control knowledge production, narrative shaping, and subject modulation. By their digital actions, the government attempted to create a submissive and predictable populace by eroding their rights to privacy and self-determination. The third process, the configuration of platform users by platform companies, concentrates on how the platform providers themselves acted in the process of counterpower movements against the government. The study examines this pattern of relationships and the processes involved in these encounters such as information production, knowledge creation, profit, culture, power making, and subject configuration.

By examining these encounters, the article will build three overarching arguments related to the challenges and solutions inherent in digitally mediated horizontal and vertical relationships. First, that digital space is neither free nor neutral. It is instead a contested space among multiple actors for the production of information and knowledge, the shaping of narratives, cultural control and profit making. There is an asymmetric power relationship between the major actors in the digital space—users, government, and platform companies—meaning that not every actor in the digital space has equal leverage on the digital network. Some actors have greater rulemaking and gatekeeping power, enabling them to structure and restructure activities in and access to the digital space, whereas others lack such capacities. Second, the article problematizes the extensive state–corporate surveillance and gatekeeping role that underlies the asymmetric power relationship as a threat to the emergence and growth of critical mass and the democratic polity. Control over the digital structure enables governments and corporations to adjust and filter the flow, processing and use of information as well as access to the digital space, thereby modulating the capacity of citizens for self-governance, self-development, and hence self-determination. Third, the article argues that challenges are aggravated when government surveillance and regulatory interests intersect with those of platform companies, which are primarily interested in profit maximization. I will elaborate on this problem of corporate complicity with governments through the legal analysis of Ethiopia's hate speech proclamation No. 1185/2020.

Examining the configuration of subjects[22] through the complicity of state–corporate power is a global challenge not limited to Ethiopia, and this article places its observations in a broader context of redefining rights to privacy. I argue that a broadly defined yet context-specific and sensitive right to privacy would guard subjects against the configurations of state–corporate power and address challenges without losing the benefit of platform technologies. This would be done by refocusing the liberal political concept of the privacy of the autonomous self onto the protection of a socially and culturally constructed and newly emergent self. In doing so, it would ensure the protection of the capacity for critical subjectivity and self-determination.

Information on vertical and horizontal digital encounters can be gathered from publicly available digital footprints left by users and mass

movement websites. The discussions in this section draw on literature from legal studies,[23] media studies,[24] sociology,[25] and political philosophy.[26] Ethiopia's digitally assisted counterpower movements are rarely studied in a structured and comprehensive manner. Although some scholarly works on Oromo protests have been published since 2014, there is almost no study that examines the relational patterns among people, government, and platform technologies in the digital spaces and its implication for the emergence of democratic self-determined society during that process. Without reiterating what has already been studied on protests and anti-government movements in Ethiopia, this article attempts to comprehensively assess only digitally mediated mass movements, looking at the patterns of the encounters between major actors and the role of platform technologies.

Pattern Mapping: Ethiopia's Technologically Mediated Movements between 2015 and 2021 and Social Media Platforms as Contested Space

This section introduces the main digitally mediated mass movements and patterns of the power versus counterpower relationship among different actors. In doing so, it depicts the nonneutrality and the contested features of the digital platform. As argued by scholars, the digital platform is a space for knowledge and the production of information by different actors, and hence a contested space for narrative setting, shaping, and the modulation of subjects and platform users.[27] In this context, power versus counterpower in digital encounters represents competition for the construction and deconstruction of meaning in the human mind through mass communication and mass self-communication.[28] Digital rivalry therefore targets people's perception of governance as well as the economic, political, and sociocultural institutions under which they live and relate to, as well as their collective identity within that sphere.[29]

Platform technologies played a crucial role in Ethiopia's power versus counterpower encounters between 2015 and 2021. This period can be described as a unique historical moment in which a critical mass disrupted Ethiopia's closed media environment by carving out its own alternative space using social media platforms. Activists and public intellectuals made use of

the digital platform to articulate peoples' demands, rights, and expectations from the government. Through wide access to and sharing of information, people become informed and helped inform their fellow citizens about their rights and responsibilities as well as failures from the government side to deliver on its duty to protect, respect and fulfil fundamental socioeconomic, civil and political rights. The relationship of power versus counterpower follows two directions, vertically against the government and horizontally as a form of rivalry between social group networks (or, to be more precise, ethnic groups).

In the vertical encounters, various social networks confronted the government and attempted to shape agendas, narratives, and disclose abuses on the ground according to their cultural, political, and socioeconomic interests and allegiances. In the vertical encounter, the major demands against the Ethiopian government between 2015 and 2018 took the form of quests for accountability, democracy, and a government that would respect laws, socioeconomic justice, civil and political liberty, and fundamental rights and freedoms.[30] Although protests took place in different regions of the country, the #OromoProtest was the most important counterpower movement. The #OromoProtest demands included a quest for socioeconomic justice including equitable resource allocation, a halt to land grabs, civil and political liberty (including the release of political prisoners and the restoration of peace), respect for human rights, and the right to self- and shared-rule.[31] To some extent, these demands were shared and reflected by other counterpower protests from ethnic groups such as the Sidama, Somali, Afar, and Amhara. The demand for group and individual rights to self-determination based on the constitutionally recognized right to self- and shared-rule of nations and nationalities was primarily advocated by the Oromo, Sidama, and other southern nations and nationalities. Their demands could be summarized as claims for access to the necessary resources for human growth that included physical well-being and intellectual, cultural, and political participation and self-determination.

In the post-2018 period, the critical mass of the counterpower movement shifted to the virtual space. The political change that had appeared so promising in 2018 turned into the same repressive system as the pre-2018 EPRDF regime in less than a year. This was followed by the aggravated deterioration

of human rights conditions and media freedom, a mismanaged and failed transition to democracy, atrocities, war crimes and crimes against humanity in Tigray,[32] and the infamous 2021 election.[33] These events galvanized and reshaped grievances against the government, broadening and complicating people's demands. As protest and resistance on the ground became almost impossible due to government repression, activists and supporters of diverse causes started to use social media platforms more aggressively by organizing Twitter campaigns and composing slogans for each campaign. The targets of these campaigns were not limited to national agencies or government organs, but were also communicated transnationally by tagging various powerful foreign institutions, individual politicians, civil society organizations, regional and international organizations, and influential diasporas in Western and Eastern countries.[34] Demands were made using digital resources and campaign websites such as the #OromoProtest and #TigrayGenocide.[35]

Meanwhile the government, threatened by the emergence of such a critical mass, reacted coercively. Its response to the digitally mediated counterpower movements between 2015 and 2021 took several forms, including violent crackdowns,[36] cyberattacks on activists' and public intellectuals' social media and other digital accounts,[37] invasive mass surveillance, and internet and communications blackouts.[38] In addition, legislative and regulatory measures, and a declaration of state of emergency[39] that significantly curbed fundamental rights such as freedom of thought, expression, movement, and privacy, were deployed by the government.[40] Targeting and penalizing journalists, lawyers and rights advocates for online posts,[41] and more recently government-backed social media campaigns to counter campaigns against the government were also among the techniques used. This vertical state-to-people encounter marked a contest between those who sought to challenge repressive state-control and a power maximizing government seeking to suppress such challenges. State designed and state-led measures set out to subvert and narrow the space for criticality, and in doing so attempted to modulate what citizens could see and know, and how they behaved.

Technology companies, including web platform corporations, although having their own self-interest and corporate goals at heart (see "Configuration by Platform Technologies," below), provided a platform for social actors,

many of whom built networks on media platforms and competed to exercise power over other social networks. As Castells[42] elaborates, competition came in the form of agenda-setting and the construction of meaning, as well as narratives that were in line with their respective goals, whether that goal was power broking, cultural construction, profit, or influencing and challenging Ethiopia's political status quo. Castells's insights can also be used to explain horizontal digital rivalry between different social groups. Even though there was an almost countrywide digitally assisted mass movement between 2015 and 2021 in Ethiopia, the demands and narratives of the various groups involved were by no means identical. This meant that there was a pattern of horizontal rivalry and occasional cooperation between different groups campaigning against the government. Looking at Ethiopia's digitally assisted movements after 2018 offers us some precise examples of horizontal digital encounters. These include but were not limited to campaigns related to state structure and causes of national crisis with competing hashtags (such as #ProblemIsTyrannyNotEthnicity vs. #StupidEthnicFederalism) and rivalry campaigns related to the war in Tigray (such as #Tigraygenocide and #TigraiPrevails vs. #EthiopiaPrevails).

Hashtags such as #ProblemIsTyrannyNotEthnicity and #StupidEthnicFederalism were often used antagonistically to show support for ethnolingual federal state structures on one hand and campaigns against it on the other, as well as underpinning quests to restore either the unitarized or geographic-based federation of pre-1991 Ethiopia. What is crucial in this digital rivalry is that each faction represented manifestations of deep-seated ideological differences within Ethiopia based on the country's statehood and attempts to inform or orient national and transnational audiences to their ideological orientation. Some see Ethiopia as a 3,000-year-old Christian nation, whereas others see it as a 150-year-old state built through the conquest of the broader South that merged ethnically, culturally, and psychologically diverse nations into the melting pot that became modern Ethiopia.[43] The pre-1974 Ethiopia was a unitarist imperialist state under the hegemonic dominance of the Northern highland culture and language that barely recognized diversity.[44] The coming to power of the EPRDF in 1991 and the birth of the 1995 constitution stopped the unitarist state structure and broke Ethiopia away from its imperialistic unitarist past.[45] Social networks

and ethnic groups remain divided along these lines, some blaming the past unitarist imperial Ethiopia for today's asymmetric power relationship among different ethnic groups and locating the cause of crisis in the imperialistic unitarist mindset, whereas others blame the current ethnolingual federal state structure for the potential disintegration of the country. It is this historical and ideological disagreement that is manifested in the digital space.

Based on the above ideological divide (but not limited to it), there were two notable moments of horizontal collaboration and confrontation between late 2019 and 2021. The first of these was related to campaigns based on the Sidama people's demand for statehood. The Sidama are one of the ethnic groups in Ethiopia that were formerly grouped as part of the southern nations and nationalities. The Sidama people's quest for statehood started long before 2019, and reached its peak during this period, eventually being realized with a referendum held on November 20, 2019, after widespread social media campaigns, activism, and protests on the ground. The Sidama people's demand for statehood was strongly backed by pro-federalism groups in Ethiopia's constituencies, primarily by the Oromo, Somalis, and other southern nations and nationalities. However, the Sidama statehood quest and alliance was hastily opposed by Ethiopian nationalist anti-multinational federation groups, mostly urban-based Amharic speaking elites. The latter group used the statehood of Sidama as a showcase for the limitations and risks of the current federal state structure. Sidama voted for independence by an overwhelming majority.

Between 2020 and 2021, in particular after war broke out in Tigray, a horizontal digital rivalry between the supporters and opponents of this war emerged. Most supporters of the war seem to do so because of grievances against the repressive TPLF-led EPRDF regime over the past twenty-seven years. It can be argued that the TPLF is considered an architect of ethnolingual federalism in the country, which is why pro-unitarist and geographic federation supporters despise it. This can be inferred from hashtags and profile pictures they often use, such as #TPLFisaTerroristGroup, to justify the war in Tigray. The screenshots in Figure 1 show some examples of horizontal encounters between different social networks on Twitter.

As was the case in the vertical state-to-people encounter, the historical and ideological intergroup rivalries that were used to shape narratives

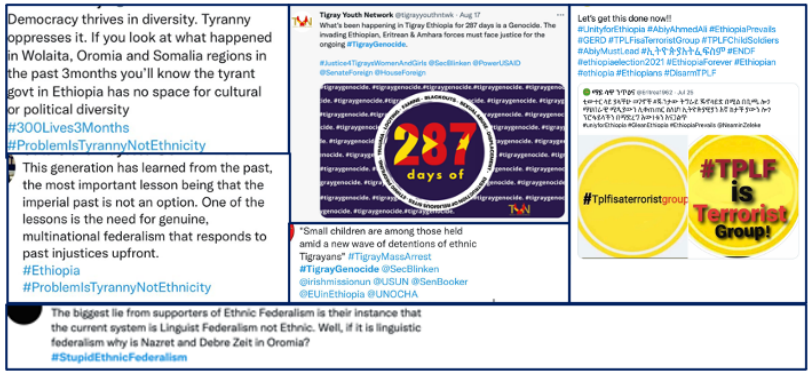


FIGURE 1. Examples of Horizontal Encounters on Twitter

through online communications are evidence of bias in the digital realm. By using platform technologies such as Twitter, different social network groups reached out to their respective audiences and constructed their own understandings and visions of Ethiopia based on the country's past, present, and future and their place and collective identity within it. Platforms in this context are neither neutral nor free. Instead they are spaces for competing narratives and identities that seek to reach as big an audience as possible and shape, reshape, construct, and deconstruct information, knowledge, and collective identity.

In both vertical and horizontal patterns of encounters, the power versus counterpower relationship represents a rivalry for configuration, knowledge and the production of information, as is the case in most other counterpower movements.[46] However, this is a double-edged sword. On the one hand, it can be argued that platform-enabled horizontal competition in the marketplace of ideas and information can contribute positively to the emergence of critical mass and a democratic society. On the other hand, as shown by recently leaked Facebook files,[47] it also carries risks such as the spread of misinformation, the invasion of privacy, and hate speech, in particular in a country like Ethiopia where there are so many contested narratives. Although careful and balanced regulation could mitigate these challenges, the added difficulty is the realization of meaningful regulation within the digital space, precisely because of the competing interests of the principal

regulating bodies, namely the government and the gatekeepers of platforms (i.e., the companies themselves) in how and why platforms are used and regulated. Hence, government policy and regulatory approaches and the business models of platform companies themselves are seldom subject- or user-centered.[48] The following section expands on these government and corporate roles and problematizes their misuse in modulating the capacity of subjects through configuration, modulation, and datafication by the converging interests of the state-platform companies.

Modulating the Capacity of Subjects: Platforms as Spaces of Configuration

In the process of horizontal and vertical encounters, governments and platforms both modulate and configure subjects to fall in line with their goals, which are primarily profit, power, and cultural expansion. In this process, the role of government as primary regulators and platform technologies as gatekeepers is paramount. Access to information, digital infrastructure, skills, and digital freedom have become crucial for the realization of human development and a democratic society. The capability for human growth goes beyond the mere legislative recognition of fundamental rights,[49] and requires access to the resources of intellectual, cultural, and political participation and self-determination.[50] In other words, making a space for critical subjects who question and assess the legal, political, socioeconomic, and cultural institutions under which they live is essential for the realization of fundamental rights and a democratic society. However, the more people are subjected to corporate and state surveillance and configuration, the less space there is for the emergence of the critical self, meaning that the capacity for democratic self-governance is diminished.[51]

This section primarily focuses on the role of the government and the platform owning companies. It problematizes the misappropriation of rule-making power and the surveillance capacity of states to prevent the exercise of basic freedom and the emergence of a critical mass, and appraises the platform companies' business models, which in general are founded on the datafication, configuration, and commodification of subjects' digital activities for capital. The section will demonstrate the asymmetric relationship

between convergent state-corporate power and platform users by using cases from the Ethiopian counterpower movement between 2015 and 2021.

Vertical Encounters and Modulation by Government

As shown in the section, "Pattern Mapping," above, social networks carve out alternative spaces on platforms to show their side of truth, in particular when the mainstream venues of representation are closed to them or dominated by the interests and narratives of dominant elites and their social networks.[52] This is particularly the case in controlled media societies like Ethiopia.[53] For instance, #Tigraygenocide and #TigrayPriveils versus #EthiopiaPriviels use social media campaign hashtags and profile pictures to campaign against the war in Tigray on the one hand and to show support for the war on the other. Likewise, campaigns such as #FreeAllPoliticalPrisoners are among broadly circulated slogans that oppose the government's repressive actions in the incarceration of opposition political leaders. People make aggressive use of platforms to draw attention to what is happening in Ethiopia because they are denied a voice in the mainstream media landscape. Digital acts that condemn the war in Tigray or political repression and the imprisonment of opposition politicians on platforms by sharing photos, footage of war and atrocities, news articles and court statements all represent processes of information production about events happening in the country, and expose rights violations that are either covered up or misreported by government and pro-government media networks.

However, access to and usage of communication platforms is neither independent nor free. Accessibility and usage is subject to control by various actors who have leverage and power over the digital infrastructure. These actors are states and platform companies, which also have their own reasons based on self-interest when making their platforms available for users. They seek to modulate and configure subjects along with their goals, such as power and profit maximization or cultural construction.[54] Governments seek to modulate citizens in line with their political programs, ideologies, goals, and interests, and by doing so preserve the status quo and maintain state domination over citizens as well as competing political, socioeconomic, and cultural actors.[55] By deploying mass surveillance, states strive to modulate the

human mind in line with government expectations and demands at a deeper level.[56] This helps governments to suppress the emergence of a critical mass that could challenge the status quo by allowing them to rely on their rule-defining and policy-making powers, and the regulatory functions through which they leverage access to media platforms and other communication infrastructures.

The Ethiopian government reacted to digitally assisted mass movements by tapping into its rule- and policymaking power as well as its regulatory function to curb access to and use of platform technologies.[57] In 2015 and 2016, the Ethiopian authorities blocked social media platforms and messaging services such as Twitter, Facebook, WhatsApp, and Viber, and openly condemned platforms for allegedly empowering "populists" and "extremists."[58] According to Access Now, between 2016 and 2021, the country shut down internet and social media platforms at least twenty times.[59] As well as invasive surveillance and internet shutdowns,[60] legislative measures were also introduced by the government to counter technologically assisted popular reprisals. The government declared a state of emergency in response to 2015–16 mass-protests[61] and recently in 2019. It also introduced a widely criticized law on hate speech and disinformation prevention and suppression in 2020, Proclamation No. 1185 /2020.[62] This law provided expansive regulatory leverage for the government on social media activities, which went as far as allowing the incarceration of individuals and leaders of online groups with more than 5,000 followers in case of misinformation and hate speech, and obliged social media platforms to take down contents that were deemed false or harmful within twenty-four hours of notification (see "The Intersection of Corporate–State Power and the Configured Subject," below).

In recent events, instead of blocking access to platforms, the government began to deploy parallel digital campaigns that competed with and countered the counterpower movement's narratives. Such state-sponsored reaction is not unique to Ethiopia. The 1997 Myanmar government's reaction to a pro-democracy movement called BurmaNet in which they instigated a parallel pro-government electronic mailing list called MyanmarNet is a similar example.[63] The Ethiopian government and pro-government networks reacted to social media campaigns that delegitimized the infamous 2021 election with hashtag #ShamEthiopianElection by organizing their own

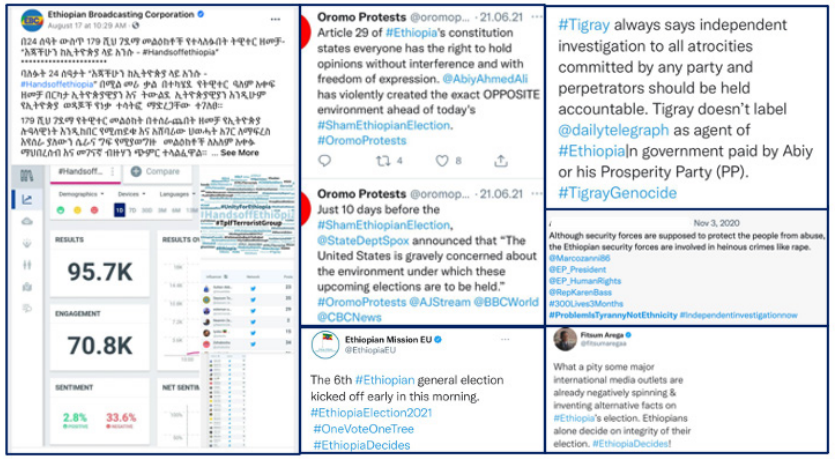


FIGURE 2. Examples of Vertical Encounters and state-sponsored Twitter campaigns

campaign version with the hashtags #EthiopiaElection2021 and #EthiopiaDecides. Government officials and supporters circulated these hashtags on Twitter. The same pattern can be observed with campaigns against the war in Tigray. The parallel digital campaign techniques went to the extent that the mainstream state-controlled media, the Ethiopian Broadcasting Corporation (EBC), prepared a segment on how to use Twitter to campaign against counterpower social media movements using what the government called "digital diplomacy."[64] Some examples of competing social media campaigns can be seen in Figure 2.

This encounter between the government and the people shows the asymmetric power relationship backed by misappropriated government regulatory, surveillance, and rulemaking leverage on the digital infrastructure, which can be seen to control access to and use of communication platforms in the interest of the government.

Configuration by Platform Technologies

Technology companies that provide platforms play a gatekeeping role by allowing access to the platform and the contents shared on it. Platform technologies, behind the apparent utopia of providing open spaces for

communities and democracy, have their own self-interests and goals, namely making a profit and shaping culture.[65] Studies show that platforms moderate human interaction, shape what we see, and govern our access and behavior, not only to protect one user from another or one group of social networks from its antagonists, but also to present their appearance to advertisers, regulators, the public, and users.[66] Platforms do this through their terms and conditions, their community standards, and via the personalization of feeds assisted by meaningful social interaction (MSI) technology and content moderation, which is performed algorithmically as well as via human input. This process helps platforms to configure human behavior and experience in line with their goals, such as promoting cultures of information and material consumption, time use, ways of communication, and perceptions of the world. This process involves the monetization of human engagement, which by extension represents the commodification of our privacy.

In principle, the idea of content moderation and the oversight of platform activities are important procedures that help mitigate hate speech and the spread of disinformation that might lead to violent incidents such as the Rohingya crisis in Myanmar[67] or the Capitol Riot in the United States.[68] Excluding those not officially reported, Facebook removed sixty-two accounts, forty-nine pages, twenty-six groups, and thirty-two Instagram accounts for inauthentic behavior and the spread of false information about the war in Tigray and other national crises in Ethiopia.[69] The most recent example of this is when the prime minister's post encouraging citizens to take up arms in defense of the government was taken down for inciting violence[70] and the Facebook Oversight Board decided to remove a post by a Facebook user related to conflict in Tigray for violating Facebook's Hate Speech Community Standard.[71] Although in part this can be seen as a positive measure, grievances against the removal of contents and the suspension of accounts without reasonable explanation have become a norm rather than an exception among activists and intellectuals involved in the digital counterpower movement of Ethiopia.

Platforms benefit from having as many users as possible, and thus portray the accessibility of their space as "open," "free," and "consensual." However, a critical examination of recent developments and information disclosed by former a Facebook employee shows the opposite. Leaked

internal Facebook files shows how the platform underregulates and has poor content moderation and safety, especially in countries such as Ethiopia. In fact, it amplifies contents that attract higher engagement using downstream MSI technology.[72] This engagement-based ranking technology predicts not what users want to see but what would spark their feelings and make them react. The rationale for using this technology to users as active and engaged as possible on the platform is profit maximization. What is often overlooked is the risk such a business model produces in fragile conditions such as Ethiopia where the platform can be used to disinform and aggravate conflict.[73]

On the other end, internet access is being promoted at the cost of surveillance and a breach of net neutrality by Facebook's Free Basics project, which has already been rolled out in more than thirty African countries.[74] The problem is that access is granted in exchange for personal data, an invasion of privacy and a risk of being profiled and microtargeted for advertising and other purposes. This criticism is often countered on the basis of consent and acceptance of platform terms and conditions by users. However, the claim ignores the fact that consent and the notion of privacy are context- and culture-specific and cannot simply be theorized through a one-size-fits-all definition of subject-centric, consent-based privacy notions. To promote such a superficial assumption, one must question the merit of consent when the alternative—to opt out—means having no other alternative than being passive subject of a repressive regime with no access to information other than that which is fed to you by the government. What alternatives do subjects in a controlled media society such as Ethiopia have when they are asked to choose between data and privacy protection and the prevention of access to a platform? This is why access to platforms does not necessarily mean that they are free or enabling. Access often comes at the expense of modulated and commodified human experience and behavior.

In the end, unless the gatekeeping role of platforms is carefully scrutinized, two types of risks may emerge. First, that platforms become the sole custodians and de facto regulators of people-to-people and government-to-people digital interactions. Second, that tech giants become complicit with repressive regimes, as is the case in Vietnam where Facebook and Google are accused of complicity with the Vietnamese government's social media censorship.[75] Regarding these risks, it is important to ask who sets

the standards against which contents are measured, and what constitutes a violation of "hate speech" or "community standards" in communities with contested historical narratives and conflicting historical memories? As shown by former Facebook employee Frances Haugen, even a human content moderation process based on user reporting must be considered seriously because people often report what they do not like rather than what is actually hateful.[76]

To sum up, the major gatekeepers of the digital space—governments and platform technologies—are both engaged in the configuration and modulation of users' experience and narrative setting and shaping for their combined best interests. What configurations by platform technologies and governments have in common is that they both use surveillance to configure and create a modulated subject programmed to be subordinate to their respective goals, whether this is political power, cultural control, or profit maximization. Through their personalized and microtargeted advertisements, platform technologies shape people's information and thus their consumption behavior and culture. Meanwhile, governments shape and modulate the behavior of their citizens through invasive surveillance and censorship that filters accessible information, and in doing so shapes knowledge about the country and its culture, identity, and governance. The cumulative effect of modulation and configuration by platform technologies and governments eventually shrinks the space for the emergence of a critical mass or people's ability to realize individual and group autonomy and self-determination. This article also argues that the greatest challenge to the emergence of a self-determined and democratic society arises when state and corporate power intersect and act complicitly. The following section examines this in closer focus, using the new Ethiopian proclamation on hate speech and disinformation prevention as a case study.

The Intersection of Corporate–State Power and the Configured Subject

At times, the powers of the two gatekeepers and regulators of the digital structure, the government and the platform-owning companies, intersect to constrain and modulate subjects, in particular when the power maximization

and narrative-shaping goals of government overlap with the profit and cultural-control goals of the platform corporation. In such instances, platform technologies act in complicity with governments to surveil and censor subjects, and by doing so shrink the space for the emergence of a critical mass. This results in the violation of people's rights to privacy, personal integrity, and self-determination.

Ethiopia's Proclamation No. 1185/2020 on hate speech and disinformation prevention and suppression was introduced as a reaction to the widespread use of platfoms and mass digital movements, and offers an example of the intersection of corporate and state power. With its vague and broad definition of hate speech (Article 2 [2]), the proclamation gives expansive regulatory power to the government and delegates censorship obligations to platform companies by requiring them to prevent the dissemination of hateful speech by the removal of all such reported content within twenty-four hours (Article 8[2]). Rights groups argue that this has a significant dampening effect on a plethora of human rights including freedom of expression, thought, access to information, and other socioeconomic and cultural rights that are affected by extension and association.[77] What is even more interesting is the government's deployment of its rulemaking leverage to create a submissive and predictable citizenry by working alongside platform companies. I refer to this as "state–corporate complicity" because despite the wide disapproval it has met with from civil society organizations, there has been no expression of disapproval and no request for clarification from social media companies against the legislative approach taken by the Ethiopian government. This despite significant gaps such as discrepancy with the legality, necessity, and proportionality requirements in the definition and content of the law.[78]

We can expand on this by looking at two major limitations. First, the proclamation obliges platforms to remove contents upon receiving notifications without saying who provided the notice or what procedures this person or body uses to underpin their demand. As far as the author knows, no challenges or questions have been raised by platform companies against such problematic obligations, despite the fact that they are in violation of their responsibility to respect fundamental human rights, which includes freedom of expression, thought, and right to privacy under the *UN Guiding*

Principles on Business and Human Rights.[79] This leaves us to assume that the notification of content removal may come from any source, including the government, based on whatever motive it chooses. Moreover, the law does not provide any precondition for notifying the user about removal of their content, nor does it offer an opportunity for judicial oversight and review. This means that the proclamation, by merging state legislative power with corporate gatekeeping leverage, effectively leaves users with no rights. The social media companies' silence in the face of such problematic legislation could be interpreted as complicity[80] with repressive regulatory regimes.

Some scholars argue that this represents the digital colonialism of social media, catalyzed by the concealed competition for exploitation of the "next billion" platform users outside the Global North.[81] Ethiopia is the second most populous country in Africa, but only 5.8 percent of its population uses social media,[82] making the country a tempting potential market for platform technologies.

The second major limitation is that there are variations in the way hate speech is defined by the community standards of platform technologies versus the proclamation. The latter adopts a definition that is broad, vague, and susceptible to subjective interpretation, and hence fails to satisfy the legality requirement. It stipulates that hate speech occurs when there is a deliberate incitement of hatred, discrimination, or an attack on a person or group based on ethnicity, religion, race, gender, or disability (Article 2[2]). On the other hand, companies such as Facebook define hate speech as "a direct attack on people based on what we call protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, caste, sex, gender, gender identity, and serious disease or disability." It is not clear what will happen when content is deemed to be hate speech under the proclamation but not under a platform's own community standards or vice versa, or which definition platform users should follow.

Furthermore, in a country with a deeply contested history and antagonistic historical memories, defining what constitutes hate, hate speech, or even disinformation is bound to be controversial. Hate and antagonism among different groups in Ethiopia are rooted in historical injustices and past asymmetric power relations.[83] Addressing historical injustice and antagonism was one the aspirational mottos of the 1995 FDRE Constitution,

which affirmed that nations, nationalities, and the people of Ethiopia aspire to build their common destiny by "rectifying historically unjust relationships and by further promoting [their] shared interests" (Preamble of 1995 FDRE Constitution). However, this remains an unfinished project, given that Ethiopia is a federation of nations still under construction. In the face of such uncertainties, criminalizing hate speech in a blanket language without full engagement with and reconciliation of past injustices is an incomplete and weak solution to a complex sociopolitical problem. What is hateful and discriminatory depends on how the targeted group perceives, sees, and relates to it—it is context-specific. For instance, would the denial of past injustices and crimes such as the Anole massacre be considered hate speech?[84] Would the abolition of the recognition of controversial figures such as Emperor Menelik II be considered hate speech? How are these and other assertions seen in the eyes of Ethiopian law and in the eyes of platform gatekeepers? As the law stands, there is no simple answer to these questions, and at best the hate speech legislation enlarges the regulatory leverage of the government over social media activities, but does little to mitigate hate speech. With intersecting corporate and state power, the space for a democratic critical mass shrinks and leads to the erosion of people's rights to self-determination.

Problems of subject modulation, configuration, shrinking space for critical mass, and capacity for self-determination are not uniquely Ethiopian phenomena. They also represent a global challenge[85] that manifests itself in the form of racial biases in AI-assisted sectors, including criminal justice and law enforcement,[86] employment and workplace management,[87] and immigration and border control.[88] Since the Snowden leaks, the trending solution for this challenge had embraced a combination of techno-legal solutions,[89] including the use of countersurveillance technologies such as encryption and surveillance self-defense tools[90] (technical solutions) and policy advocacy around legal solutions to protect privacy and personal data through the right to privacy (legal solutions). It can be argued that advocacy for the right to privacy as a gateway to safeguarding other rights and human autonomy in the digital space and beyond is gaining ground.[91] Without fully subscribing to this assertion, the following section will discuss how the legal solution of privacy rights could be used to protect the capacity for self-determination and the emergence of critical mass in Ethiopia.

Remedial Thoughts: Privacy Rights for the Protection of Self-Determination and against Configuration

The notion of privacy has been a subject of debate for a long time, and is still not settled. Despite the lack of consensus on its definition, the UN special rapporteur on the right to privacy noted that the concept of privacy is related to individual autonomy and self-determination that safeguards and enables our fundamental right to dignity and free, unhindered personal development.[92] Although this contextualization represents a good start, most mainstream interpretations of privacy rights are criticized for being individual subject-centric, narrow, and context-blind interpretations.[93] The mainstream legal understanding of the right to privacy protection is criticized for being context-blind, because it is disproportionately drawn from Western-based empirical experience,[94] and individualistic, because it overly focuses on the subject's autonomy and private life.[95] Meanwhile, other studies highlight the fact that the dominant techno-legal solutions against invasive corporate and state surveillance disproportionately focus on individual users rather than sociopolitical and economic structures[96] that have an enabling or disabling force on an individual's capacity to act autonomously—to make an independent choice and exercise meaningful self-determination in the digital space and beyond. A comprehensive critique against the association of privacy with individual interests is presented by Regan,[97] who argues that the value of privacy in promoting autonomy, human development, and freedom of thought and action must not stop at the good they bring to individuals but must include the benefits they bring by helping to create a vibrant democratic society and social institutions.[98]

In addition to the emerging appraisal of individually focused privacy narratives, scholars warn that the very notion and scope of privacy is dynamic and context-specific—meaning that it depends on society's sociocultural values and dominant political philosophy.[99] Cohen argues that this view requires detaching privacy from the liberal legal theory that has been built around the individual subject-centered protection of the autonomous self through the notion of consent. Decisions and experiences in the digital space cannot simply be theorized in terms of individual choice and consent. Individual choices and consent are also socially shaped through networks of

relationships, practices, beliefs, and embodied experiences.[100] Experiences in the digital space are shaped by background socioeconomic, political, and historical factors as well as through other dynamics against which existing power asymmetry is invisibly played out. These factors cumulatively determine people's access to, usage of, and leverage in the digital space, which puts the notion of privacy beyond individual choice and consent. This argument helps explain the limitation of characterizing privacy as a choice, and choice as a deliberately autonomous act when the alternative is hardly viable.[101] We can trace this argument back to our earlier question in digital control in Ethiopia between 2015 and 2021, namely, what alternatives do subjects in a controlled media society such as Ethiopia have when they are forced to choose between data and privacy protection and access to an alternative platform? What is the merit of consent when the alternative to opting out means becoming the passive subject of a repressive regime and having no access to information other than that which is feed to you by the government?

Based on these critical perspectives, the notion of privacy that might present at least a partial solution to the state–corporate configuration and modulation of subjects problematized above is a privacy right that nurtures collective societal values and is context-sensitive. Nissenbaum[102] argues that privacy as a right to the proper flow of personal information is contextual, or dependent on the circumstances in which an act is prescribed. Context, according to Nissenbaum, is an "abstract representation of social structures experienced in daily life." In light of this, digital encounters in Ethiopia between 2015 and 2021 can be seen as a sociopolitical space of resistance against authoritarianism, or more precisely as a resistance to the realization of individual and group self-determination, socioeconomically, politically, and informationally. Therefore, the privacy protection this article seeks draws on this sociopolitical context and circumstance.

The FDRE Constitution recognizes the right to privacy as a fundamental human right under Article 26. In addition, Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, which recognize the right to privacy, are part and parcel of Ethiopia's law of the land, its Constitution. The FDRE Constitution explicitly protects citizens against arbitrary and unlawful interference to a

person's home, person, or property, and this also encompasses correspondences and communications (Article 26[1 and 2]). Most important, Article 26(3) affirms that the state carries a duty to respect and protect this right. This is important because unlike trends in other jurisdictions, the Ethiopian Constitution imposes negative and positive duties: a duty to refrain from violating rights and a duty to protection against rights violations by third parties, such as corporations. A cumulative reading of Article 26 with Article 29 of the FDRE Constitution on freedom of expression, thought, and opinion further strengthens the social value of privacy in nurturing the emergence and growth of a vibrant, critical, and democratic citizenry.

The respect for and fulfilment of Article 29 also represent ways of realizing the positive state duty to protect under Article 26. This is mainly because if, as asserted by the special rapporteur, the right to privacy is related to a person's right to self-determination, which in turn safeguards and enables fundamental rights to dignity and free, unhindered development of the self, its fulfilment would go beyond nonviolation or negative duty. It would require the creation of an environment conducive to the realization of such a right. Among the conditions required for the realization of self-determination through privacy rights and the emergent critical self is access to uncensored information, a space for open communication and a permissive environment that encourages freedom of thought without modulation and configuration by government and technology companies. This could be fulfilled only when the government adheres to Article 29 of the FDRE Constitution, which guarantees the right to seek, receive, and impart information and ideas. Thus, that which the Constitution safeguards, based on Articles 26 and 29, goes beyond the protection of individual subjects and nurtures the emergence of critical mass by creating a conducive environment for self-development and meaningful self-determination, digitally and beyond.

Despite the rich legal and constitutional protection of privacy rights, the empirical reality in Ethiopia, as discussed above, shows the opposite. The government, in its vertical encounter with counterpower digital movements between 2015 and 2021, violated Articles 26 and 29 of the FDRE Constitution as well as the international human rights principles Ethiopia has agreed to and ratified. By deploying surveillance technologies, censorship in complicity with platform technologies, and through the abuse of its regulatory leverage,

the Ethiopian government has reneged on its duty to respect and protect. By using its regulatory and rulemaking leverage to reduce the space for freedom of thought, expression, and access to information, the government has violated its duty to respect its citizens. It has also violated its duty to protect by acting complicitly with platform technologies to modulate and configure subjects. This intersection of state–corporate configuration and modulation of subjects is contrary to international human rights standards and Ethiopia's laws, because it denies and reduces the space for self-development, critical thinking, and the conversion of human experience into commodifiable aspects of a benign society.

Building on this positive constitutional foundation, this article proposes a redefinition of the concept of privacy that would protect the human capacity for self-determination by centering a socially constructed human agency both as an individual and group. This redefined notion of privacy must be based on a framework of a broadly defined yet context-specific rights to privacy that first enable self-development, second protect a socially and culturally constructed emergent self, and third allow the capacity for self-determination.

The notion of privacy rights that enable self-development entails both a positive and a negative duty on states and corporations. The negative duty obliges the state and other organs not to interfere with the individual exercising of self-development through activities such as but not limited to self-learning, thought sharing, discussion, and participation in public debates. Moreover, to encourage the realization of self-development, individuals will need resources. Therefore, a privacy right that enables self-development goes beyond protection against interference or a simple negative duty. It entails a positive duty of states and technology industries to fulfil the material and nonmaterial conditions necessary for the realization of personal development. Among these conditions is access to an infrastructure of uncensored information, freedom of thought, expression, and capacity for independent decision making. State and corporate censorship amounts to restraint in accessing relevant information through which individuals could otherwise inform and improve themselves, thereby suppressing our capability for self-development.

In examining the privacy rights to protect a socially and culturally constructed emergent self, as advised by Cohen, our understanding of "self" and "private" needs to take a broader perspective beyond individual subject-centric notions. "Self" and "private" are socially and culturally constructed concepts. What is private for some sections of the community maybe not so private for others. Meanwhile, the notion of "self" varies across cultures; there is no uniform understanding of self among the individualistic societies of the Global North and the more communal societies in the Global South. For example, the Ubuntu philosophy that states "I am because we are" is more deeply entrenched in the interconnectedness of humanity than it is in the individual self. This study therefore argues that privacy must be rooted in subjects' lived experiences rather than exist as a predefined notion of privacy, autonomy, and the self. We must understand that what is private and what is not, and who may access what aspects of our lives and for what purpose, are socially and culturally constructed concepts. People and their perceptions are constructed, as is the level of leverage and autonomy they have over infrastructure such as the digital space—meaning that access to and usage of this space is subject to political, cultural, and social systems.

The fulfilment of self-development and protection for the socially and culturally constructed self will eventually create a space for nurturing the emergence of critical mass and hence the capacity to informed self-determination. This means the inclusion of a privacy right that protects and allows an environment and a space in which to inform oneself and critically reflect while rooted in a proper understanding of people's lived experience, creating a vibrant, democratic, and critical mass through the capability to determine what is best for oneself as an individual and collectively as a group.

Conclusion

Based on empirical observations of the digitally mediated counterpower social movements in Ethiopia between 2015 and 2021, this article has examined the patterns of relationships and encounters among the main actors in the digital space—the users, the government, and platform-owning companies. This observation has shown how the major players in the digital space are all engaged in rivalry to shape narratives, and to configure and

modulate subjects and social networks in line with their respective goals. Although acting as consumers of platform technologies and being subject to configuration by governments and platforms, users also compete to construct narratives, information, and knowledge about socioeconomic policies, political narratives, and collective identities in their horizontal encounters. This observation highlights the competition for the shaping of contested historical narratives and political views in Ethiopia between different groups.

The study also problematized platform technologies and the government's use of their gatekeeping power to the digital infrastructure through surveillance, rulemaking, and regulations that configure and create a modulated subject programmed to be subordinate to their power making, cultural construction, or profit maximization goals. Using the example of Ethiopia's hate speech Proclamation No. 1185/2020, this article also showed how corporate and state power can intersect at times to disable subjects. The article argues that the cumulative effect of modulation and the configuration of platform users by platform technologies and the government eventually shrinks the space for the emergence of critical mass and the capability of people to realize their individual and group rights to self-determination. The study concluded that Ethiopia's deployment of regulatory leverage, censorship, and surveillance technologies in complicity with platform technologies violates the right to privacy and freedom of thought protected under the FDRE Constitution as well as Ethiopia's commitment to the standards of international human rights.

To address this challenge, the article proposes a redefined notion of privacy rights that goes beyond mainstream individual subject-centered and context-blind notions of privacy. It proposed a redefined privacy right that would enable self-development, and would protect a socially and culturally constructed emergent self, and the capacity of that self for critical subjectivity and self-determination as an individual and as part of a collective.

This interdisciplinary and empirical case-based assessment of digitally assisted counterpower movements and the role of major actors contributes to the existing body of knowledge in at least two ways. First, its particular focus on digitally assisted counterpower movements in Ethiopia and the relationship patterns involved in this process examines an area that is not yet well-explored. Even though there have been several studies on counterpower

movements in Ethiopia, there are almost no empirically supported studies that investigate the relationship among actors in the digital space and their impact upon the emergence of critical mass. Second, even though the article based its empirical assessment on Ethiopia, the remedial thoughts it develops can also be generalized as an input and may be applicable beyond the specific case of Ethiopia. The legal assessment of privacy recognized under international human rights law makes the proposed solution potentially relevant for other jurisdictions. As future research agenda the study tables further investigation into how digital media is shifting from tools to demand greater political accountability and reform to ammunition for supporting competing projects in an open conflict.

Notes

The author thanks the special issue editors and anonymous reviewers for their helpful comments and review.

1. Iginio Gagliardone, *The Politics of Technology in Africa: Communication, Development, and Nation-Building in Ethiopia* (Cambridge: Cambridge University Press, 2016).
2. Yohannes Eneyew Ayalew, "The Internet shutdown muzzle(s) freedom of expression in Ethiopia: competing narratives," *Information & Communications Technology Law*, 28, no.2 (2019): 208–224.
3. "Platform" throughout this article is used to mainly refer to social media platforms.
4. "Occupy Together," *Occupy Together*, September 25, 2011, https://web.archive.org/web/20130514230107/http://www.occupytogether.org/.
5. La Redacción, Jorge Araizaga, and Rosalia Vergara, "Se Globaliza #Yosoy132; Cuenta Con 52 Células En Distintas Partes Del Mundo," *Proceso*, August 3, 2012, https://web.archive.org/web/20131230233429/http:/www.proceso.com.mx/?p=315804.
6. "Indignados/15M Movement Collection from Spain", *Digital PUL*, 2011, https://dpul.princeton.edu/15m.
7. "BurmaNet," *BurmaNet*, December 31, 2005, https://web.archive.org/web/20171231233454/http://www.burmanet.org/news/.

8. "Arab Spring: History, Revolution, Causes, Effects, and Facts," *Encyclopedia Britannica*, January 27, 2021, https://www.britannica.com/event/Arab-Spring.
9. "BlackLivesMatter Global Network," *BlackLivesMatter*, 2013, https://blacklivesmatter.com/.
10. John Arquilla, and David Ronfeldt, "The Advent of Netwar (Revisited)," in *Networks and Netwars*, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND Corporation, 2001), 1–26.
11. W. Lance Bennett, and Alexandra Segerberg, "The Logic of Connective Action," *Information, Communication and Society* 15, no. 5 (2012): 739–68.
12. Manuel Castells, *Networks of Outrage and Hope: Social Movements in the Internet Age* (Malden, MA: Polity Press, 2012).
13. Manuel Castells, "Network Theory: A Network Theory of Power," *International Journal of Communication* 5 (2011): 15.
14. John Markakis, *Ethiopia: The Last Two Frontiers* (Woodbridge, UK: BOYE6, 2013).
15. Tatek Abebe, "Lost Futures? Educated Youth Precarity and Protests in the Oromia Region, Ethiopia," *Children's Geographies* 18, no. 6 (2020): 584–600.
16. "A Government Plan, a People's Protest and a Government's Response," *Amnesty International*, March 2017, https://www.amnesty.org/en/latest/campaigns/2017/03/ethiopia-state-of-emergency-violates-human-rights/; "Miracle or Mirage? Manufacturing Hunger and Poverty in Ethiopia," Oakland Institute, September 15, 2016, https://www.oaklandinstitute.org/miracle-mirage-manufacturing-hunger-poverty-ethiopia.
17. These are leaders, members, and supporters of opposition political leaders since the coming to power of Abiy Amhemed's government under the Prosperity Party, e.g., leaders and members of the Oromo Liberation Front, Oromo Federalist Congress, and Balderas for Genuine Democracy.
18. "Ethiopia: Troops and Militia Rape, Abduct Women and Girls in Tigray Conflict, New Report," *Amnesty International*, August 10, 2021, https://www.amnesty.org/en/latest/news/2021/08/ethiopia-troops-and-militia-rape-abduct-women-and-girls-in-tigray-conflict-new-report/.
19. "Imperfect Elections Do Not Fortify Ethiopia's Transition," Chatham House International Affairs Think Tank, June 17, 2021, https://www.chathamhouse.org/2021/06/imperfect-elections-do-not-fortify-ethiopias-transition.

20. Awol Allo, "Protests, Terrorism, and Development: On Ethiopia's Perpetual State of Emergency," *Yale Human Rights and Development Law Journal* 19 (2017): 46; Téwodros W. Workneh, "Ethiopia's Hate Speech Predicament: Seeking Antidotes Beyond a Legislative Response," *African Journalism Studies* 40, no. 3 (2019): 123–39; Abebe, "Lost Futures?"
21. "Facebook" is used throughout this article primarily because most examples and discussions in the article are cases that took place before Facebook changed its name to Meta.
22. The term "subjects" is used to refer to platform users and only rarely used to imply citizens.
23. Julie E. Cohen, "Turning Privacy Inside Out," *Theoretical Inquiries in Law* 20, no. 1 (2019): 1–31, https://doi.org/10.1515/til-2019-0002; Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, CA: Stanford Law Books, 2009).
24. Paolo Gerbaudo, and Emiliano Treré, "In Search of the 'We' of Social Media Activism: Introduction to the Special Issue on Social Media and Protest Identities," *Information, Communication and Society* 18, no. 8 (2015): 865–71; Emiliano Treré, "Reclaiming, Proclaiming, and Maintaining Collective Identity in the #YoSoy132 Movement in Mexico: An Examination of Digital Frontstage and Backstage Activism through Social Media and Instant Messaging Platforms," *Information, Communication and Society* 18, no. 8 (2015): 901–15; Lina Dencik, Arne Hintz, Joanna Redden, and Emiliano Treré, "Exploring Data Justice: Conceptions, Applications and Directions," *Information, Communication and Society* 22, no. 7 (2019): 873–81.
25. Castells, "Network Theory"; David Lyon, "Surveillance, Power and Everyday Life," in *Emerging Digital Spaces in Contemporary Society: Properties of Technology*, ed. Phillip Kalantzis-Cope and Karim Gherab-Martín (London: Palgrave Macmillan), 107–20.
26. Payal Arora, "Decolonizing Privacy Studies," *Television and New Media* 20, no. 4 (2019): 366–78.
27. Julie E. Cohen, "Configuring the Networked Citizen," in *Imagining New Legalities: Privacy and Its Possibilities in the 21st Century*, ed. Austin Sarat, Lawrence Douglas, and Martha Merrill Umphrey (Stanford, CA: Stanford University Press, 2012), 129–53; Julie Cohen, "Cyberspace As/And Space," *Georgetown Law Faculty Publications and Other Works*, no. 1 (2007), https://

scholarship.law.georgetown.edu/facpub/807; Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (New Haven, CT: Yale University Press, 2018); Ulises A. Mejias and Nick Couldry, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford, CA: Stanford University Press, 2019).

28. Castells, "Network Theory."
29. Gerbaudo and Treré, "In Search of the 'We' of Social Media Activism"; Lorenzo Coretti and Daniele Pica, "The Rise and Fall of Collective Identity in Networked Movements: Communication Protocols, Facebook, and the Anti-Berlusconi Protest," *Information, Communication and Society* 18, no. 8 (2015): 951–67.
30. Abebe, "Lost Futures?"
31. Allo, "Protests, Terrorism, and Development"; "The Morning After: The Oromo Option(s) and the Imperative of Agonistic Engagement," *Kichuu* [blog], August 27, 2018, https://kichuu.com/the-morning-after-the-oromo-options/.
32. "Ethiopia."
33. "Imperfect Elections Do Not Fortify Ethiopia's Transition,"
34. Claire Wilmot, Ellen Tveteraas and Alexi Drew, *Dueling Information Campaigns*, *The War Over The Narrative In Tigray* (The Media Manipulation Casebook, 2021), https://mediamanipulation.org/case-studies/dueling-information-campaigns-war-over-narrative-tigray.
35. "Oromoprotest," 2019, https://oromoprotests.org/; "About Us—Omna Tigray," *Omna Tigray*, November 4, 2020, https://omnatigray.org/about-us/.
36. "Ethiopia: Beyond Law Enforcement: Human Rights Violations by Ethiopian Security Forces in Amhara and Oromia," *Amnesty International*, May 29, 2020, https://www.amnesty.org/en/documents/document/?indexNumber=afr25%2f2358%2f2020&language=en; "A Government Plan."
37. Bill Marczak, Geoffrey Alexander, Sarah McCune, John Scott-Railton, and Ron Deibert, "Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware," *The Citizen Lab*, December 6, 2017, https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/.
38. "Ethiopia: Freedom on the Net 2016 Country Report," *Freedom House*, 2016, https://freedomhouse.org/country/ethiopia/freedom-net/2016; "Ethiopia: Freedom on the Net 2017 Country Report," *Freedom House*, 2017, https://

freedomhouse.org/country/ethiopia/freedom-net/2017; "Ethiopia: Freedom on the Net 2018 Country Report," *Freedom House*, 2018, https://freedomhouse.org/country/ethiopia/freedom-net/2018; "Ethiopia: Freedom on the Net 2019 Country Report," *Freedom House*, 2019, https://freedomhouse.org/country/ethiopia/freedom-net/2019; "Ethiopia: Freedom on the Net 2020 Country Report," *Freedom House*, 2020, https://freedomhouse.org/country/ethiopia/freedom-net/2020.

39. "Freedom House—Source Description,"*Ecoi.Net*, April 8, 2020, https://www.ecoi.net/en/source/11154.html.
40. "A Government Plan"; "Ethiopia: End Arbitrary Detentions of Tigrayans, Activists and Journalists in Addis Ababa and Reveal Whereabouts of Unaccounted Detainees," *Amnesty International*, July 12, 2021, https://www.amnesty.org/en/latest/news/2021/07/ethiopia-end-arbitrary-detentions-of-tigrayans-activists-and-journalists-in-addis-ababa-and-reveal-whereabouts-of-unaccounted-detainees/.
41. Amnesty International, (2021) 'Ethiopia', 12 July 2021
42. Castells, "Network Theory."
43. Mohammed Hassen, *The Oromo of Ethiopia: A History 1570–1860* (Trenton, NJ: Red Sea Press); Markakis, *Ethiopia*; Martha Kuwee Kumsa, "At Issue: Learning Not to Become Oromo—Chasing the Ghosts Chasing John Sorenson," *Northeast African Studies* 9, no. 3 (2002): 161–92; Merera Gudina, *Ethiopia: Competing Ethnic Nationalisms and the Quest for Democracy, 1960–2000* (Addis Ababa, Ethiopia: Shaker Publishing B.V.).
44. Kassim Shehim, "Ethiopia, Revolution, and the Question of Nationalities: The Case of the Afar," *Journal of Modern African Studies* 23, no. 2 (1985): 331–48.
45. Tsegaye Regassa, "State Constitutions in Federal Ethiopia: A Preliminary Observation," *Statecon.Camden.Rutgers.Edu*, 2004, 12,https://statecon.camden.rutgers.edu/sites/statecon/files/subpapers/regassa.pdf.
46. Tiffany Danitz, and Warren P. Strobel, "Networking Dissent: Cyber Activists Use the Internet to Promote Democracy in Burma," in *Networks and Netwars*, ed. John Arquilla and David Ronfeldt. The Future of Terror, Crime, and Militancy (Santa Monica, CA: RAND Corporation, 2001), 129–70, https://www.jstor.org/stable/10.7249/mr1382osd.10.
47. Eliza Mackintosh, "Facebook Knew It Was Being Used to Incite Violence in Ethiopia. It Did Little to Stop the Spread, Documents Show—CNN," *CNN*,

October 25, 2021, https://edition.cnn.com/2021/10/25/business/ethiopia-violence-facebook-papers-cmd-intl/index.html; "The Facebook Files," *Wall Street Journal*, October 1, 2021, sec. Tech, https://www.wsj.com/articles/the-facebook-files-11631713039.

48. Kate Klonick, "The New Governors: The People, Rules, and Processes Governing Online Speech," *Harvard Law Review* 131 (2018): 73.
49. Martha Nussbaum, "Capabilities as Fundamental Entitlements: Sen and Social Justice," *Feminist Economics* 9, nos. 2–3 (2003): 33–59.
50. Cohen, "Turning Privacy Inside Out."
51. Cohen, "Turning Privacy Inside Out."
52. Castells, *Networks of Outrage and Hope*.
53. Terje Skjerdal, and Sintayehu Gebru, "Not Quite an Echo Chamber: Ethnic Debate on Ethiopian Facebook Pages during Times of Unrest," *Media, Culture and Society* 42, no. 3 (2020): 365–79.
54. Castells, "Network Theory"; Gillespie, *Custodians of the Internet*; Mejias and Couldry, *The Costs of Connection*.
55. Danitz and Strobel, "Networking Dissent."
56. Lina Dencik, Arne Hintz, and Jonathan Cable, "Towards Data Justice? The Ambiguity of Anti-Surveillance Resistance in Political Activism," *Big Data and Society* 3, no. 2 (2016).
57. Gagliardone, *The Politics of Technology in Africa*.
58. Paul Schemm, "In Ethiopia's War against Social Media, the Truth Is the Main Casualty," *Washington Post*, October 14, 2016.
59. "Open Letter to Prime Minister Abiy Ahmed Ali: Keep the Internet Open and Secure throughout the Upcoming Elections and Thereafter," *Access Now*, June 18, 2021, https://www.accessnow.org/keepiton-open-letter-ethiopia-election-2021/.
60. "Ethiopia: New Spate of Abusive Surveillance," *Human Rights Watch*, December 6, 2017, https://www.hrw.org/news/2017/12/06/ethiopia-new-spate-abusive-surveillance.
61. "Legal Analysis of Ethiopia's State of Emergency," *Human Rights Watch*, October 30, 2016, https://www.hrw.org/news/2016/10/31/legal-analysis-ethiopias-state-emergency.
62. "Ethiopia's Hate Speech and Disinformation Law: The Pros, the Cons, and a Mystery," *Access Now* [blog], May 19, 2020, https://www.accessnow.org/

ethiopias-hate-speech-and-disinformation-law-the-pros-the-cons-and-a-mystery/.

63. Danitz and Strobel, "Networking Dissent."
64. የቲውተር ዘመቻን እንዴት መቀላቀል ይቻላል?, *EBC,* 2021, https://www.youtube.com/watch?v=ePykGrtIDqY&ab_channel=EBC.
65. Gillespie, *Custodians of the Internet*; Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* 30, no. 1 (March 2015): 75–89.
66. Gillespie, *Custodians of the Internet*.
67. "Myanmar: Human Rights Groups Call into Question Facebook's Role in Rohingya Crisis," *Business & Human Rights Resource Centre*, October 30, 2017, https://www.business-humanrights.org/en/latest-news/myanmar-human-rights-groups-call-into-question-facebooks-role-in-rohingya-crisis/.
68. Eric Schewe, "After the Capitol Riot, Who Will Govern Speech Online?," *JSTOR Daily*, February 4, 2021, https://daily.jstor.org/after-the-capitol-riot-who-will-govern-speech-online/.
69. "Removing Coordinated Inauthentic Behavior From Ethiopia," June 16, 2021, https://about.fb.com/news/2021/06/removing-coordinated-inauthentic-behavior-from-ethiopia/.
70. Associated Press, "Facebook Removes Ethiopian PM's Post for Inciting Violence," *Voice of America*, November 4, 2021.
71. Facebook, "Oversight Board Upholds Meta's Original Decision: Case 2021-014-FB-UA," *Oversightboard.Com*, December 2021, https://oversightboard.com/news/927673894608838-oversight-board-upholds-meta-s-original-decision-case-2021-014-fb-ua/.
72. "The Facebook Files."
73. Sarah Howard, "Underinvestment, Corporate Greed and Lack of Oversight: The Scandal of Facebook's Role in Ethiopia's Conflict," *African Arguments*, December 1, 2021; Roland Polman, "Facebook Is Fanning the Flames in Ethiopia," *The Continent*, no. 64 (2021): 16–17.
74. Nothias Toussaint, "Access Granted: Facebook's Free Basics in Africa," *Media, Culture and Society* 42, no. 3 (2020): 329–48.
75. "Tech Giants Complicit in 'Industrial-Scale' Repression in Viet Nam," *Amnesty International*, December 1, 2020, https://www.amnesty.org/en/latest/news/2020/12/viet-nam-tech-giants-complicit/.

76. Kate Linebaugh, and Ryan Knutson, "The Facebook Files," *The Journal—WSJ Podcasts, Part 7: The AI Challenge*, October 19, 2021, https://www.wsj.com/podcasts/the-journal/the-facebook-files-part-7-the-ai-challenge/318d6439-93e5-4352-9f08-402af9a79d4b.
77. "Ethiopia: Bill Threatens Free Expression," *Human Rights Watch*, December 19, 2019, https://www.hrw.org/news/2019/12/19/ethiopia-bill-threatens-free-expression; "Ethiopia: Hate Speech and Disinformation Law Must Not Be Used to Suppress the Criticism of the Government," *Article 19*, January 19, 2021, https://www.article19.org/resources/ethiopia-hate-speech-and-disinformation-law-must-not-be-used-to-supress-the-criticism-of-the-government/.
78. "United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression, David Kaye Visit to Ethiopia: End of Mission Statement," *Office of the United Nations High Commissioner for Human Rights* [OHCHR],December 2–9, 2019, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25402&LangID=E.
79. "Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework," January 2012, *UNOHCHR*, https://www.ohchr.org/en/publications/reference-publications/guiding-principles-business-and-human-rights.
80. Florian Wettstein, "Silence as Complicity: Elements of a Corporate Duty to Speak Out Against the Violation of Human Rights," *Business Ethics Quarterly* 22, no. 1 (2012): 37–61.
81. Payal Arora, *The Next Billion Users: Digital Life Beyond the West* (Cambridge, MA: Harvard University Press); Arora, "Decolonizing Privacy Studies."
82. "Digital in Ethiopia: All the Statistics You Need in 2021," *DataReportal—Global Digital Insights*, 2021, https://datareportal.com/reports/digital-2021-ethiopia.
83. Kassim Shehim, "Ethiopia, Revolution, and the Question of Nationalities: The Case of the Afar," *Journal of Modern African Studies* 23, no. 2 (1985): 331–48.
84. Mohammed Hassen, "Conquest, Tyranny, and Ethnocide against the Oromo: A Historical Assessment of Human Rights Conditions in Ethiopia, ca. 1880s–2002," *Northeast African Studies* 9, no. 3 (2007): 15–49.
85. Lyon, "Surveillance, Power and Everyday Life."
86. Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* (Medford, MA: Polity Press, 2019).

87. Umoja Noble Safiya, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York: New York University Press).
88. Mirca Madianou, "Nonhuman Humanitarianism: When 'AI for Good' Can Be Harmful," *Information, Communication and Society* 24, no. 6 (2021): 850–68.
89. Dencik et al., "Towards Data Justice?"
90. "Surveillance Self-Defense," *Surveillance Self-Defense*, 2022, https://ssd.eff.org/en.
91. "The Right to Privacy in the Digital Age: Report," September 15, *OHCHR*, 2021, https://www.ohchr.org/EN/Issues/DigitalAge/Pages/cfi-digital-age.aspx.
92. "Report of the Special Rapporteur on the Right to Privacy" *Human Rights Council*, A/HRC/31/64, November 24, 2016, 10.
93. Kebene Wodajo, "Mapping (In)Visibility of Structural Injustice in the Cyberspace," *Journal of Responsible Technology* 9, 100024.
94. Arora, "Decolonizing Privacy Studies."
95. Cohen, "Turning Privacy Inside Out."
96. Dencik et al., "Towards Data Justice?"
97. Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill: University of North Carolina Press, 2000).
98. Regan, *Legislating Privacy.*
99. Alan F. Westin, "Social and Political Dimensions of Privacy," *Journal of Social Issues* 59, no. 2 (2003): 431–53.
100. Nancy S. Kim, *Consentability: Consent and Its Limits* (Cambridge: Cambridge University Press).
101. Benjamin, *Race after Technology*; Payal Arora, and Laura Scheiber, "Slumdog Romance: Facebook Love and Digital Privacy at the Margins," *Media, Culture and Society* 39, no. 3 (2017): 408–22.
102. Nissenbaum, *Privacy in Context*, 134.

Kebene Wodajo is a postdoctoral fellow at the Institute for Business Ethics, University of St. Gallen. She can be reached at kebene.wodajo@unisg.ch.