Cartographies of digital dissidence: Networked movements, Internet laws, and Internet Ungovernance Forums in Turkey and Brazil
by Zeyno Ustun

Abstract
Networked movements play a critical role in resisting political intimidation. Two such mobilizations that coincided in June 2013, Turkey’s Gezi Resistance and Brazil’s Vinegar Uprising, illustrate the tactical and strategic utilization of the Internet. Tellingly, Internet laws were amended in the aftermath of both events. While Turkey’s law took the direction toward an authoritarian digital geography for its user-citizens, Brazil’s *Marco Civil da Internet*, first seen as an ideal legal text, did not circumvent commercialization of the local network. While Internet laws were amended in the light of digital capacities revealed by networked movements, Internet Governance Forums — held in Turkey in 2014 and Brazil in 2015 — similarly aimed to dispose of digital dissidence, staging an uncanny alliance between transnational digital platforms and local central authorities. In response, counter-events occurred in Turkey and Brazil, entitled ‘Ungovernance Forums’. Though the Internet has been celebrated as a democratic architecture of information governed by universal protocols, this paper sheds light on how digital dissidents have been trapped in a tension between governance of the Internet and jurisdictional claims of nation states over their digital geographies. Lost in the popular discourse of the Internet providing a self-governing platform for social communication, have we missed the opportunity to imagine a future? Are we faced with the prospect of a hyper-securitized Internet that instead produces cartographies of authoritarian control that promise not a distributed and generative milieu but the very opposite?

Contents
1. Introduction
2. Methodology
3. A critical framework on digital dissidence
4. Claiming digital geography via Internet laws
5. “Behind the farce of global multi-stakeholder(ism)”
6. Conclusion

1. Introduction

The same game is now being played over in Brazil ... the symbols are the same, the posters are the same, Twitter, Facebook are the same, and the international media are the same. They are being led from the same center. They are doing their best to achieve in Brazil what they could not achieve in Turkey. It’s the same game, the same trap, the
same aim. — Recep Tayyip Erdogan, quoted in Cohadzic (2013).

The simultaneous mobilizations in June 2013 in Turkey and Brazil demonstrated a great deal about the ground rules of digital geography and the threats digital dissidents face in the twenty-first century. Several authors have noted that the Internet plays a significant role in contemporary social movements. Many have glorified the capacities of free, open, and distributed communication that the Internet seems to offer to all social classes (Hardt and Negri, 2012; Castells, 2012; Gerbaudo, 2012), while few warn of its potential use to exert control, even as information communication technologies are increasingly utilized against protesters (Tufekci, 2017; MacKinnon, 2011). There is, however, a lack of scholarly investigation into the political and legal aftermath of networked movements while accounting for local digital infrastructure. The movements in Turkey and Brazil, each successful global media events with international audiences, failed to produce tangible outcomes as protesters faced similar political and legal consequences, despite sharp differences between the two respective administrations. This article focuses on the aftermath of networked movements and explores how, when faced with popular digital dissidence, each country claimed their digital geography via institutional and regulatory maneuvers, formed an alliance with transnational commercial platforms, and incrementally exerted central control over critical infrastructures of the Internet.

The Internet is a space of resistance and repression, all at the same time. In the aftermath of simultaneous movements that coincided with the NSA revelations in 2013 (see, for example, MacAskill and Dance, 2013), the Internet was revealed as a complex space in which multiple forms of power operate all at once. In 2016, the U.S. formally recognized cyberspace as a domain of war, alongside air, land, sea, and space, with NATO members following the year after (Zittrain, 2017). The simultaneous movements served as important turning points for both Turkey’s and Brazil’s Internet, as it was revealed the two countries were categorized as ally-targets by the NSA. Since 2013, along with deteriorating political atmospheres in both countries, the cartographies of resistance have been under constant duress and patrol of centralizing mechanisms of control. Understanding how traditional forms of state power operate over this newly appointed political geography, therefore, has the utmost contemporary relevance in assessing the risks that digital dissidents face.

In this study, via a methodology I call cartographic ethnography, I demonstrate how central authorities in two nation states, each late-comers to the digital field, sabotaged the democratic potential of digital dissidence. Applying theories of social movements, infrastructuralism, and legal theory together, I analyze the ways in which regulatory control of the local Internet conflicts with standards that characterize its global governance and display how digital dissidence falls under the thumb of central administrative bodies that operationalize deepening forms of networked authoritarianism (MacKinnon, 2011).

To do so, I discuss the two social movements as longitudinal processes and explore how both Turkey and Brazil responded to them, paying particular attention to the legal activities that ensued. Contextualizing it against the changing debates on Internet governance and the challenge of Ungovernance Forums, I argue that national law aligns with the critical infrastructures of the Internet, vertically forming a legal layer and changing the conditions of networked movements radically. The legal layer establishes centralizing mechanisms of control over local traffic online, repressing the distributive qualities of the Internet that other technical, communicational, and physical layers were designed to maintain. Therefore, a vertically aggressive layer in the multi-layer model of the global Internet can better account for the contradictions of digital partition and jurisdiction and the intensifying risks that digital dissidents face based on their geolocation.

2. Methodology

This article draws not only from my scholarship but also my activism. Influenced by scholars of digital ethnography (Burrell, 2009; Lingel, 2017; Barassi, 2013), I developed a multi-modal methodology that I call cartographic ethnography by which I make use my own experiences as a digital dissident in the Gezi resistance.

Qualitative network analysis has flourished thanks to Latour’s actor-network theory. The social for Latour can only be studied and understood “in a very peculiar movement of re-association and re-assembling” and a “complex interconnection between human and non-human agents” [1]. Such an inquiry that maps out relationships manifesting as a “parliament of things” requires innovative methods and tools that enable the researcher to navigate among multiple sites and timelines. Barassi (2013) offered a new concept that she labeled ‘ethnographic cartography’. Combining multi-modal methods of data collection, such as participant observation, textual analysis, and interviews,
she studied the everyday experience of the networks of Cuba Solidarity Campaign (CSC; see https://cuba-solidarity.org.uk) — a British organization embedded within the Labour Movement — and investigated the way in which political alliances and affinities were constantly constructed, challenged, and re-constructed. Barassi’s focus, however, was on the human components of the social network (Barassi, 2013). While she regards social movement networks as processes of human negotiation and interaction, what I suggest with cartographic ethnography in this study aims at understanding social and technical networks as spatial and temporal processes subject to a variety of processes. In this study, this means understanding changing material conditions as well as digital activism and political retaliation.

Cartographic ethnography involves studying the digital infrastructure of networked movements up close and accounting for their human and non-human components, as well as their multilayered architectures. Burrell (2009) argues taking networks as field sites produces a continuous space that does not presume proximity or even spatiality in a physical space. Rather the ethnographer is embedded in a site composed of fixed and moving points including spaces, people, and objects (Burrell, 2009). Lingel (2017) similarly states “networked field studies require mobility, not only in terms of investigating separate communities and technologies, but also in accounting for both online and offline practices, and tracing the different platform, devices and sites that emerge within a communitys socio-technical milieu.” I follow their approaches as a network that require mobility and immersing oneself to moving parts and connections. I take these simultaneous movements as shared sites of networked mediation and of building transnational solidarity.

I gained first-hand experience in both movements and their consequences. In the summer of 2013, as a member of the Taksim Solidarity, an umbrella platform consisting of 128 constituent groups that triggered networked resistance in Gezi Park, Istanbul, I organized with digital dissidents of the Gezi Resistance. Taksim Solidarity was immediately indicted for inciting masses to violence via social media. Over the following seven years, the platform was ultimately indicted and acquitted twice by courts.

In 2014, I was invited to the 32nd São Paulo Biennial in Brazil to hold a cartography workshop with local media activists. I also privately interviewed Ronaldo Lemos, professor at the Law School of Rio de Janeiro State University, a key figure behind the bill regulating Brazilian online activity, Marco Civil da Internet. Returning to Turkey, I attended workshops of Alternative Informatics, an association that worked on issues around information technologies in Turkey and initiated the Ungovernance Forums that would be held in Turkey and Brazil. Through my experience with digital activists, law makers, technology and media workers in both countries, I learned how the law can be used to control the local Internet and how it thereby failed to provide a free and open space for new forms of political action or protect groups associated with networked movements. I saw how similar the grievances and means of resistance online were in each country, as well as the violence by security forces on the streets and the Internet.

In addition to my participation in Turkey and Brazil as an activist over the last seven years, I also study the conditions of contestation online via the universal-technical codes that make up their shared digital space of resistance, the local legal amendments to Internet laws following protests, and the international political factors that shaped the governance of the Internet. My research also benefits from the use of digital tools to collect sources on the Web and map my subject matter. I use the infrastructure of Graph Commons (https://graphcommons.com), a collaborative mapping platform for which I have been a researcher since 2011, in order to map the issues on Internet governance on one canvas, focusing on debates in the UN-led Internet Governance Forums (IGF) from 2006–2018 and Ungovernance Forums that contested IGF in 2014–2015.

3. A critical framework on digital dissidence

3.1. Two movements, one Internet?

An array of new social movements erupted around the world in the twenty-first century. While some shared political triggers, most were united against the effects of advanced capitalism. Unemployment, exploitative work, accelerated urban transformation, authoritarian leadership, and ecological disasters were among the shared grievances that the movements manifested (Dyer-Witheford, 2015). The Gezi Resistance in Turkey and the Vinegar Uprising in Brazil started in the cities of Istanbul and São Paulo in early June 2013. Constituting the first mass movements of this scale in both countries for three decades, the grievances of protesters centered on systemic gentrification and dispossession of urban populations.
Butler (2014) discusses how tempting it has been for those who observed the 2013 protests from afar to include the Gezi Resistance among the cluster of protests called the “Arab Spring.” Arguing that it has become increasingly difficult to agree on the conditions of their sameness, if they ever existed, she asked “how far can that generalization go, does it matter if states are governed by a different security logic?” Contemporary social movements indeed confront the effects of advanced capitalism as a common enemy and the symptoms were evident in both cases that I study here. In a similar vein to Butler, however, I argue for examining the simultaneous movements in Turkey and Brazil in a relationship, rather than pursuing mere comparisons or conditions of sameness. Approaching the two movements in a reflexive fashion, therefore, I take my own path as a digital dissident as one of the many connections made between the two geographies that attracted immense attention to the Internet as a battlefield. In the aftermath of June 2013, furthermore, not only did our experiences as activists provided a basis for reading the two movements together, but so did the amendments to respective Internet laws following the popular dissent in both countries and the International Governance Forums which travelled to Turkey and Brazil in 2014–2015.

The first wave of networked movements — including the Arab revolts, European anti-austerity mobilizations in Greece and Spain, and Occupy Wall Street in the U.S. — generated a universal repertoire of digital contention (Tilly, 2006; Castells, 2012). Protesters in Turkey and Brazil learned from earlier digital dissidents how to reach wider social networks and organize the masses as broadcast media were blocked out during massive protests in Istanbul and São Paulo. Coinciding with the Snowden revelations in June 2013, simultaneous movements in Turkey and Brazil were in a second wave of networked movements that likewise allowed central authorities the time to learn from recent history. The Internet was immediately acknowledged and targeted as a space of resistance by both governments.

Facing country-wide, popular contestation as well as external surveillance, the administrations of Erdogan and Rouseff amended respective Internet laws. The two administrations were in sharp difference in terms of their styles of governance. The motivation behind new legislative actions were accordingly different. Nonetheless, the experiences of digital dissidents had been similarly shaped around the same ‘security logic’ that reigned in cyberspace in the aftermath of the two movements. Threatened by simultaneous movements, both Brazil and Turkey initiated processes for the hyper-securitization and hyper-commercialization of the Internet that changed the face of national digital geographies as well as the experiences across the two cartographies of digital dissidence. The resonance and dissonance between them deserve further study.

3.2. Networked authoritarianism

The regulability of the Internet has been long debated by legal scholars. While some dismiss the effectiveness of national laws arguing in favor of the resilience of standards, protocols, and the network effect, some insist that the Internet has been already fragmented over the last two decades, not only into linguistic and cultural territories but also into nationally defined topologies of control. In this section, from the vantage point of digital dissidents, I will deliver a critical framework on networked authoritarianism, discussing theories of and around Internet laws, governance, and media infrastructures.

Scholars who picked up the widely popular vision that the Internet was essentially unregulable claimed that the cyberspace is “a civilization of the mind” and argued that it is a separate jurisdiction in which the laws of real life do not apply. This vision entailed that the codes and protocols of the Internet would remain unchecked by geographic borders or state-specific regulations. Cohen (2012) argued that technical code did not, however, displace the presumption of geographic separateness that animated legal scholarship about “cyberspace”. Cyberspace for him cannot be taken as an immaterial virtual space that has detached the mind from the corporeal being of the person, whose body after all is subject to the jurisdiction of nation states; “it is people in real space who want and need information, and for whom neither perfect freedom nor perfect control holds sustained attraction.” Bernal (2018), in a similar vein, reflected on the claims made by some scholars that insisted that earthbound rules could apply to cyberspace, labeling them as cyberlibertarian. As Bernal pointed out, though this seems attractive and reasonable to many at the first glance, the cyberlibertarian view has major flaws in its imagination over the actual nature of cyberspace. Even though a person’s online identity may operate outside borders, Bernal argued, in line with Cohen, that their physical body exists in a physical place where real-world governments hold power.

There is a second group of scholars that Bernal examined, cyber-paternalists who arose in continuation and reaction to libertarians. Following similar normative and practical aspects, these scholars argued that the government should intervene not at the regulatory level but at the level of technical code; those who created and operate the Internet need to embed ‘values’ in the technology. A merger between state and public innovation at the level of the nation state is, however, antithetical to the history of the Internet. As Zittrain (2017) reminded us, only some major governments...
are uniquely positioned, through the power of coercion entailed by national sovereignty, to insist upon changes to software or even hardware deployed on key private platforms.

Divorcing legal code from technical at the national level however seems practically impossible. It is likewise impossible to ‘immaterialize’ bodies and see individuals as an abstraction, as merely users, when it comes to defining the Internet as a political geography partitioned into nation states. Framing Internet governance as technical only, as Radu (2019) argued, obliterates related social-political implications and minimizes latent political stakes [2]. Radu stated that the global governance of the Internet systematically combined various dimensions of state and non-state regulation and different modalities to operate at the level of setting the rules of the game. She argued that the global governance framework presents us a ‘bricolage’ picture of coordination, modeling, and routine interactions at regional, local, and global levels (Radu, 2019).

Since the late 2000s, however, a number of scholars have warned of a process of fragmentation of the global Internet governance, particularly in light of Russian and Chinese networks. Investigating ‘Great Firewall of China’ in 2011, MacKinnon (2011) argued that “there are difficult issues of government policy and corporate responsibility that must be resolved in order to ensure that the global Internet and mobile technologies can fulfill their potential to support liberation and empowerment” [8]. She explained that when threatened authoritarian governments learn quickly and build capacity to control digital communications networks. Coining the phrase networked authoritarianism, MacKinnon identified in the case of China, common tactics in the form of repressive control mechanisms, including networked cyberattacks, device and network controls, domain-name controls, localized disconnection and restriction, and astroturfing and public outreach. Maréchal (2017) argued that compared to China’s favoring limits to access, Russia relied on censorship and intimidation, while investing in a ‘kill switch’ as a means of infrastructural control in case of crises. Maréchal noted that Russia normalized and helped to spread networked authoritarianism through various strategies in Internet governance activities, at the UN, and through the Shanghai Cooperation Organization “authoritarians’ club” [9].

As Kohl and Fox (2017) argued, however, after the NSA revelations, the nation state has been asserting itself across the globe, that cyber-borders based on national law are not just erected around China’s or Russia’s online communities, but even in the West. “Those cyber borders through which states work to carve out their autonomy in the online world”, they state, “are for most intents and purposes invisible to the ordinary users whose experience of the Internet continues to be relatively seamless” [10]. Within the tensions between networks of digital dissidence and authoritarian rule online, however ‘intents and purposes’ are far from being invisible, even for ‘ordinary’ users. Since 2013, in fact, both in Brazil and Turkey digital dissidents have been subject to draconian security measures and a longitudinal retaliation process, as were critical infrastructures of the Internet.

A new material perspective is needed to understand the kind of political geography that cyberspace represents, to evaluate the practical effectiveness of existing regulatory methods of information control across nation states, and to examine the critical relations and normative affinities formed between local authorities and the governance framework, as well as transnational corporations.

3.3. Horizontal versus vertical partitioning

Stating that the issue of the fragmentation or splitting up the Internet was more of an inflammatory one, Mueller (2017) argued that the fragmentation debate is really a power struggle over the future of sovereignty in the digital world. The threat for Mueller was not a threat toward technical fragmentation of the Internet per se; rather it has been about geopolitics, national power, and the future of global governance [11]. Mueller offered a new perspective to the sovereign claims of nation states over their digital geographies. He argued that an assertion of authority by a given state over local configuration constituted alignment (Mueller, 2017). Mueller writes:

“Alignment is the digital equivalent of building customs checkpoints, tariffs, and roadblocks into the network — with the proviso that in the digital environment the effects of any locality’s barriers will be felt globally as well as locally.” [12]

With the concept of alignment, in other words, Mueller stated that the exertion of central power appeared not as a technical reshaping of the local network, but as creating new mechanisms and institutions of control, aligning with infrastructure. A form of sovereignty was created for the globally distributed Internet that encouraged each nation state to mistrust and restrict access to capabilities that have not been approved, certified, or developed nationally. He identified methods of control and argued that national securitization involved (1) the recognition of cyberspace as a
Almost two decades ago, Galloway and Thacker (2004) situated mechanisms of control for which they coined the term "protocological control" to define a new form of power that operates over decentralized (horizontal) and multilayered (vertical) systems. In digital geographies, like that of the street, they discussed that control over networks which manifests itself as crowd control, surveillance, and military blockading, while implemented at the level of protocols. Derived from computer science, protocol is interpreted by Galloway and Thacker as a totalizing control apparatus that guides both technical and political formations of networks. Different from previous modes of social and technical organization such as hierarchy or bureaucracy, for Galloway and Thacker, “as a technology, protocol is implemented broadly and is thus not reducible simply to the domain of institutional, governmental, or corporate power. In the broadest sense, protocol is a technology that regulates flow, directs netspace, codes relationships, and connects life forms” [14]. All these domains are layered networks, overlapping and conflicting with one another.

In a similar vein, Bratton (2016) used the Stack, another concept borrowed from computer science, to situate sites and modes of control in a multi-layer design model of digital communications. Drawing from Carl Schmitt’s work of the Nomos of the Earth studying political subdivisions of Earth (of land, seas, and/or air, and now also the domain that the U.S. military simply calls “cyber”), Bratton says the Stack, is the new nomos rendered now as vertically thickened political geography [15]. Unlike Westphalian horizontal borders that define the sovereignty of nation states, Bratton argued that the Internet is in fact partitioned by vertically stacked software and hardware. Bratton identified six layers that make up this megastructure: Earth, cloud, city, address, interface, and user. The foundational layer of the Internet is naturally the Earth itself. The cloud layer is the second to rise and derives energy and minerals from the Earth to store universal information in massive data centers, while the city layer is the technological urban scape that “captures humans and consoles them within walls” of surveillance (Bratton, 2016). The technical address layer is composed of numerical as well as linguistic addresses designated via standards and protocols to everything that we find online. The interface and user layers are communication layers that ensure translation between machine-generated language and human semantics (Bratton, 2016).

Bratton’s Stack offers a critical perspective in seeing the Internet as a kind of political geography “with the horizontal subdivision of physical sites by and for states, but also according to the vertical stacking of interdependent layers on top of one another: two geometries sometimes in cahoots, sometimes completely diagonal and unrecognizable to one another” [16]. Particularly focused on the cloud and user layers, Bratton discussed the Sino-Google conflicts of 2008 to the present (Bratton, 2016). To him, this was a clash between two logics of governance, two geometries of territory that continue to grind against the grain of one another. Bratton noted:

“... It is not at all clear whether, in the long run, Cloud platforms will overwhelm state control on such flows, or whether states will continue to evolve into Cloud platforms, absorbing the displaced functions back into themselves, or whether both will split or rotate diagonally to one another, or how deeply what we may now recognize as the surveillance state (U.S., China, and so forth) will become a universal solvent of compulsory transparency and/or a cosmically opaque megastructure of absolute paranoia, or all of the above, or none of the above.” [17]

The stack provides an abstract model for examining complex multi-layered geometries of geopolitics today, the two logics of governance — that of state and non-state actors of sovereignty — seem to reign in separate domains of jurisdiction. As the two cases studied in this article demonstrate the ways in which the two logics of governance, that of nation state and transnational corporate platforms, are not only compatible but interfaced. The legal and political aftermath of the simultaneous movements empirically display how in the case of Turkey the centrifugal institutions, and in the case of Brazil, economic concessions to non-state actors of the cloud resulted in networked control and repression.

The legal configurations at the level of the nation state — that accommodate various human activities from labor to dissent — does not only change how information flows, how it is filtered and barricaded, but also changes how agency is distributed over networks, intensifying the risks that digital activists face. If we take the nomos of the global digital space as rendered a vertically thickened political geography, I argue a vertically aggressive legal layer, that the nation state rules, disrupts the operations not only at the technical and address levels of the megastructure, but also successfully aligns with platforms of the cloud layer (Bratton, 2016; Mueller, 2017).

military domain and reframed cybersecurity as a problem of national security; (2) territorialization of information flows; and, (3) alignment of critical Internet resources (Mueller, 2017) [13].
Navigating over the cartographies of digital dissidence interwoven between Turkey and Brazil, I now present two cases in respect to national configurations, and contestations to them, focusing on multi-vectorial relationships between digital dissidents, nation states, transnational corporations, as well as international bodies like discussion forums that host critical debates around the Internet.

4. Claiming digital geography via Internet laws

A cartographic critique can help clarify common forms of digital retaliation that digital dissidents face, across layers of digital geography at the level of the nation state. This can be seen in both the Turkish and Brazilian cases as the two movements triggered a process of political retaliations in both countries in the aftermath of simultaneous movements.

Major political events have taken place in both countries since 2013 as Turkey and Brazil experienced significant political escalations. While Erdogan’s AKP (Adalet ve Kalkınma Partisi or Justice and Development Party) reinforced its state power by constitutional amendments and survived a coup attempt organized by Gülen movement in 2016. In Brazil, President Rousseff, representing the the Worker’s Party (Partido dos Trabalhadores or PT), was impeached in a trial that many saw as a legal coup d’état [18]. Today, Erdogan’s deepened authoritarianism since 2016, undeniably provides a stronger basis for comparison with the post-2016 rule in Brazil, particularly with the current Bolsonaro administration, a far-right president with a military background. Facing contention from a former ally, Erdogan used intensifying methods of digital retaliation as counter-terror police targeted Fethullah Gülen-linked media, the same outlets that once helped Erdogan attack the opposition (Bulut, 2016). Bolsonaro, in tension with the opposition party, steered Brazil’s Internet down to bold technological authoritarianism, violating all that Marco Civil da Internet was hoped to democratize, by a decree compelling all federal bodies to share most of the data they hold on Brazilian citizens, and consolidate it into a vast master database, Cadastro Base do Cidadão (Citizen’s Basic Register) [19].

However, as I argued earlier, I take the simultaneous movements as significant turning points that not only reinforced the Internet as a space of resistance and control, but also triggered critical debates on the democratic potentials of digital communications technologies trans-locally and multifocally across national and international networks. In this claim on the cartographies of digital dissidence in two geographies, hyper-securitytization, in the Turkish case, and hyper-commercialization, in the Brazilian one, changed the face of the national digital geographies.

4.1. Turkey’s Internet surveillance law

In its January–July 2016 transparency report, Twitter noted that Turkey had made the largest number of requests to block users [20]. This was during the same six-month period in which 1,656 Twitter users in Turkey were arrested (Yesil and Sözeri, 2017). In fact, there has been a steady uptick in the degree of repression executed by the AKP regime since the 2013 Gezi movement swept the country. Having survived powerful contestation, the AKP government swiftly organized itself within the very same networks as its dissidents, politically and legally pressuring transnational platforms. This became first apparent in September 2014, when the AKP government passed amendments to the Internet Act via Communication Law No. 5651 (Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publications; see https://wipolex.wipo.int/en/legislation/details/11035), later known as Turkey’s “Internet surveillance law.” [21]

Amendments to Law No. 5651 triggered outrage across dissident networks, particularly since the law enhanced AKP’s authoritarian grip. Directly tied to the Prime Minister, the Internet Act restricted access to Web sites in record speed, as short as four hours, via techniques of DNS-based and URL-based Web site blocking [22]. The law also established a centralizing unit within the regulator ICTA (Information and Communication Technologies Authority or Bilgi Teknolojileri ve İletişim Kurumu [BTK]), responsible for imposing bans and blocks on Web sites. With the European Court of Human Rights ruling that Law No. 5651 was in violation of the European Convention on Human Rights, Turkey’s amendments triggered further protests that criticized a draconian attitude to using the Internet for horizontal communication and organization. Law No. 5651 allowed Turkey’s telecommunications authority to block Web sites and censor Internet content without court decisions. This forced Internet service providers to maintain records of user activities for two years and make them available to authorities when requested, without notifying users. Realizing that digital geography could be claimed and manipulated to secure it from existing and potential dissidence, the AKP government therefore “annexed” the local Internet in Turkey via amendments to the Internet Act, introducing ICTA and centralizing all ISPs (Internet Service Providers) (Akgül and Kirdoğ, 2015).
From 2014 to the end of 2019, access to a total of 408,394 Web sites was blocked, according Akdeniz and Güven (2020) for a report published by the Freedom of Expression Association (Ifade Özgürlüğü Derneği, IFÖD) in Turkey. After URL-based blocking was introduced in February 2014 with Article 9 of Law No. 5651, a total of 16,358 news URLs were blocked and the content of 8,523 sites was removed. These reports were banned by a total of 4,158 decisions.

The AKP regime operationalized a deepening form of networked authoritarianism at the level of a vertically aggressive legal layer (MacKinnon, 2011). These tactics aimed at dismantling cartographies of resistance, defeating groups for whom survival heavily relied on networked solidarity to remain informed on the well-being of one another as a means to form some sense of resilience against political authority. The Erdogan administration successfully blocked traditional media thanks to RTUK (Radyo ve Televizyon Üst Kurulu, Radio and Television Supreme Council), which tellingly was assigned to monitoring streaming services available via the Internet, with a law issued in August 2019.

If regulability refers to the government’s capacity to control behavior within its reach, administrative regulation by the Internet’s sovereign legal power disrupts all networking capacities, eliminating protesters who lack the necessary know-how or digital literacy to keep combatting online. In other words, despite the technical shortcomings of legal decrees in face of the dynamics of technological innovations, local laws altered the ground rules of digital geography as a space for resistance in Turkey, particularly paralyzing the democratic potential to utilize the Internet for a popular and durable networked movement.

4.2. Brazil’s bill of Internet rights; Marco Civil da Internet

In April 2014, Brazilian President Dilma Rousseff announced the issuance of Marco Civil da Internet in the opening speech of the Global Multi-stakeholder Meeting on the Future of Internet Governance (Net Mundial) [25], held in Brazil. In effect a declaration of independence of the Brazilian Internet, the law was written through a participatory process for which activists had long fought. Though Rousseff’s government had kept the bill on her desk for four years, Marco Civil became the highlight of Net Mundial 2014, with Rousseff additionally staging a two-day event about NSA monitoring of her phone and e-mail messages [26].

During my 2014 visit to Brazil, I met privately with the bill’s creator, Ronaldo Lemos. Delivering the essentials significant to stakeholders and upholding issues around copyright that commercial lobbies had pushed for, negotiation was central to the process, in his view, of generating an ideal deal that compromised along the way. He saw Net neutrality as the first result of the negotiations, heralding a provision of equal data packets without regard to the content, origin, or destination, service, terminal, or application, as guaranteed in Article 9. Privacy of personal data came next, included to offset abusive online platforms, with Articles 10-23 ensuring that all storing, sharing logs and other activity relevant to “personal data and the content of private communications should preserve the intimacy, private life, honor, and reputation of the parties directly or indirectly involved” (Knight, 2014). “On November 5, 2014, however, a new version of the draft law of the Civil Rights Framework for the Internet in Brazil — Marco Civil da Internet, PL 2126 of 2011 — was submitted to the Chamber of Deputies. It outlined the government’s concerns in light of the Snowden affair, authorizing the Federal Government to require ISPs and content providers to store the information of all Brazilian users” (Knight, 2014).

One year after this compromise to a seemingly ideal law, the Internet Governance Forum was held in Brazil on the theme of Internet Governance: Empowering Sustainable Development. This time, Rousseff signed and publicly endorsed Facebook’s Internet.org, violating for many the provisions of the Internet legislation that she had passed earlier (Knight, 2014).

Meeting with Facebook CEO Mark Zuckerberg, Rousseff signed Brazil as a member country to Zuckerberg’s personal project Internet.org, invoking widespread outrage across cartographies of resistance in the country. In theory, Free Basics by Facebook (https://connectivity.fb.com/free-basics) was to provide individuals with access to useful mobile services in markets where Internet access was less affordable. Its Web sites, available for free without data charge (zero-rating), included news of current events, employment, health, education, and local information. By introducing people to the Internet’s benefits, it aimed to bring them online and improve their lives, “in hopes that one day, everyone will be connected” (Internet.org).

Internet.org infrastructurally trapped the citizen/user/protester inside Facebook by selling only mobile data and by zero-rating that mobile data if the user primarily used the digital platform to access the Web. The alliance between the contractee for-profit platform and the contractor government left the latter unaccountable for fiber optic cables,
Internet service, cheap connectivity, and so forth. In other words, the project brutally commercialized digital geography to the degree that its potential tactical use was significantly undermined. Nation states, despite the peculiarities that surface when it comes to partitioning digital geography, are clearly effective in vertically controlling traffic online in the local. In the Turkish case, central bodies that are in cooperation with digital platforms securitized the content online by surveilling, filing, and pursuing digital dissidents. In Brazil, commercialization of the cyberspace defied the generative qualities of the Internet by commissioning its service and facilitation to for-profit transnational platforms.

5. “Behind the farce of global multi-stakeholder(ism)’

At the same time as the Turkish and Brazilian Internet laws were taking shape, the UN-led Internet Governance Forum (IGF), convening first in Turkey (2014) and then in Brazil (2015), rejected all applications coming from protesters who had participated in networked movements, despite advertising itself as open to all Internet stakeholders. Once this became clear, a parallel event titled the Ungovernance Forum was held in protest, first in Istanbul and then in São Paulo [27], with participation by international dissidents like Jacob Applebaum and Julian Assange [28].

5.1. Internet Governance Forums

As an UN-led global gathering convening since 2005 to discuss pressing problems around global connectivity, the Internet Governance Forum (IGF) brings people together through annual conferences of various stakeholder groups discussing public policy issues related to the Internet.

Even though the global meetings serve as discussion bodies, not involved in decision-making, the Internet Governance Forum provides a space of trans-local discussion, and “while there is no negotiated outcome, the IGF informs and inspires those with policy-making power in both the public and private sectors.” [29] Most importantly, the 2014 and 2015 forums, travelled to Turkey and Brazil, assembling national and international networks of engineers, business actors, state figures, and various other stakeholders in the aftermath of massive country-wide uprisings that were also global media events that attracted significant audiences in the Global North and South. Both forums, therefore, were conceived as a legitimate platform of dialogue by the networks of digital dissidents, seen as opportunities to speak about critical issues around governance patterns.

Radu described a periodization of specific governance patterns, identifying three phases of Internet governance: “(1) the early days of the Internet dominated by informal governance and focused on technical standards (1970s to 1994); (2) the globalization of the Internet closely linked to increasing roles of private actors and the salience of the market-oriented approach (1995–2004); and, (3) the decade of global regulatory arrangements (2005–15) delivering hybrid configurations to the fore, privileging cross-sectoral partnerships.” Post-2015, however, Radu argued, new power trends indicated a stronger position for a limited number of companies and states [30]. Her classification is useful, reinforcing Western-based narratives of the making of the global Internet, thus the late addition of countries to the debate, when pressing issues are dominated by a powerful few.

Using digital tools, I scraped the archive of IGF conferences and reorganized significant topics addressed by the chairs of each conference in the countries where events took place. These themes had been generated by local chairs of IGF annual meetings, who assumed responsibilities for funding meetings. Scraping revealed similarities and sharp differences as the venues navigated across different countries.

In Figure 1, the network map shows the core problems identified by the chairs of each year’s conference. The three clusters — Before the Networked Struggles, During the Movement and the Aftermath — trace topics from before the emergence of networked movements to the period of active mobilization and its aftermath.
Cartographies of digital dissidence: Networked movements, Internet laws, and Internet Ungovernance Forums in Turkey and Brazil

Figure 1: Internet movements.

Topics identified by the host country each year demonstrate that the debates that seem to cruise along with changing technologies and their impact on information technologies in the Global South. While themes like privacy, diversity, and access retain their significance over changing use and meaning of global connectivity, other issues become peripherally important, like gender, cybersecurity, or cloud computing. Themes such as access, privacy, and management of critical Internet resources bridge issues that connect two clusters revealed on the diagrammatic canvas as clusters of two broad periods: 2006–2013 and 2013–2018. Openness and diversity were essentials of the first period, whereas human rights and cybersecurity became central issues of the second.

Not surprisingly, IGF 2014 and IGF 2015 parallel one another in terms of issues collapsed under the theme of human rights. Given that both countries experienced a similar push from stakeholders that was mostly concerned with the dismissal of democratic practices, it is telling that all applications coming from groups active in these movements were rejected by the IGF.

5.2. Internet Ungovernance Forums
5.2.1. Ungovernance Forum Turkey

The Ungovernance Forum, a platform conceived to challenge the perceived shortcomings of the IGF, was an offshoot of the association Alternative Informatics (Alternatif Bilişim Derneği) [31]. I became acquainted with it in 2011, when the AKP introduced the first wave of amendments to Law No. 5651. The ensuing “Don’t Touch My Internet” rally, largely organized by Alternative Informatics, shared the news of massive resistance to proposed changes across the international arena. I joined it as part of my preliminary field research, when the association organized a summer camp in Izmir, Turkey in July 2015. I attended the program as a participant observer, watching as it evaluated the Ungovernance Forum as a counter-event and laid out its prospective vision in the struggle for a just and open Internet in Turkey.

Alternative Informatics justified the Ungovernance Forum because “it is more imminent than ever to strengthen networks of solidarity and connect struggles across the globe for the Internet we want.” [32] It envisioned the forum as “a space in which we can discuss the problems and solutions of the Internet openly, with courage, and without shying away from conflict.” [33] With the Ungovernance Forum, the organizing committee aimed to hijack the guest pool of the UN-led event IGF. The counter-event garnered massive international attention.

A welcome text conveyed the resentment and fear of delegitimization that had motivated the organizers. Written in a tone of emergency that acknowledged the contingencies of the moment, it urged its international audience to recognize that the Turkish government had reached out to Silicon Valley, with the result that “Facebook and Twitter are now censoring political activists and citizen journalists.” “Turkey is not unique,” the forum argued, highlighting “a direct connection today between how states and corporations treat people and our natural resources; the discontent expressed across main squares of the world, and the struggles against surveillance and censorship.” [34]

It identified three fronts for resistance. The common denominator of all three divides was an emphasis on the value of digital dissidence for understanding the global distribution of information and the struggles that it generated, modes that would not be duped by assumed divisions between materiality and immateriality, national and transnational power domains, or legal and technical codes. In other words, the protesters positioned themselves against digital platforms who would not assist them in offsetting political intimidation in Turkey, appealing to citizen-users instead who generated content.

5.2.2. Ungovernance Forum Brazil

The Ungovernance Forum was repeated the following year in Brazil, when networks of digital dissidence circulated a press release for their own Ungovernance Forum in August 2015 [35]. Organized after all of their submissions were rejected by the IGF, the forum highlighted the insincerity of the IGF’s reliance on the term “multi-stakeholder” and argued that its meetings in fact served transnational corporations and local governments in forming alliances to the exclusion of local dissidents. Its text noted that “it has become obvious that Internet governance is a farcical way of keeping us busy and hiding a sad reality.” It lamented that “nothing concrete in these 15 years, not a single action, ever emerged from multi stakeholders meetings, while at the same time technology as a whole has been turned against its users as a tool for surveillance, control and oppression.” [36]

Brazil’s Ungovernance Forum also advocated that global citizens think about the critical challenges ahead. Following the call of the original counter-event in Istanbul, the São Paulo counterparts made a call to “end mass surveillance, protect freedoms online without compromise, guarantee Net neutrality, and enable universal access to the free Internet.”

All four forums, governance and ungovernance, benefited from a vibrant media environment in both countries that the networked movements cultivated. Not only digital dissidents, but also a critical mass, were interested in the ways in which the Internet had been changing. Tellingly, IGF travelled to Turkey and Brazil in consecutive years to harvest what the movements triggered, yet rejected all applications coming from protesters. UN-led conferences, in other words, took a clear stand against multi-stakeholder(ism) that they have been advertising since the global sessions were inaugurated in 2006.

Behind the farce of multistakeholderism, IGF, as yet another body filtering critical debates, controlled the assembly of a public platform in ways that were consistent with local authorities, a terrifying display of policing debates and excluding digital dissidence. While a vertically aggressive legal layer in both countries aimed for a structural dismissal of any contestation online, whether it has been via draconian measures or via commissioning digital geography to transnational platforms, IGF followed and reinforced the lead of local political authorities and their normative
structures in governing the local Internet. Unruly alliances surfaced, in other words, that mobilized central
governments, transnational digital platforms, and international bodies against the tactical repertoire of political action
online.

---

6. Conclusion

This article has shown how networked movements using the Internet have been tactically constrained by the material
infrastructure of digital geography. Though international and transnational forces have at times cooperated with
national ones, examining the horizontally distributed yet vertically thickened (Bratton, 2016) digital geography
displays a far more contradictory and disturbing picture (Mueller, 2017). This multimodal qualitative analysis was
conducted to show what was shared across two geographies as well as provide a kaleidoscopic picture of cartographies
of resistance.

The Internet is after all simultaneously a space of resistance and repression. Alliances between authoritarian
governments and transnational tech corporations, displayed in the cascade of parallel mobilizations in Turkey and
Brazil, have prevented the emergence of more inclusive and democratic relations of power on the Internet, despite its
centrality to the new logic of political action for networked movements in the twenty-first century. Unlike broadcast
media, the Internet does not suffer from direct control or regulation of its bandwidth. However, across technical and
legal processes described here, the Internet has been revealed as a highly commercialized and securitized geography in
the hands of centralizing national and international bodies. Their legal-administrative grip established control of digital
traffic locally, endangering cartographies of digital dissidence and causing dissident networks in both Turkey and
Brazil to be barricaded structurally, surveilled, defamed, delegitimized, and in many cases incarcerated.

A legal layer was inserted to claim digital geography at the national level, a layer that is vertically aggressive to the
universally standardized technical layers of the Internet, trapping users/citizens in spaces of not only commercial but
authoritarian surveillance. Researchers and scholars of the Internet must account for local-legal codes that force
cartographies of dissidence to fall under the thumb of nation-states. Administrative manipulations of critical
infrastructures of communication makes it difficult to talk about a global Internet while posing a profound threat to the
free and just distribution of social communication across countries and territories globally.

Digital dissidents will keep carving out cartographies of resistance online, particularly with new subversive
technologies of communication that they engineer. However, the future for networked social movements depends on
digital dissidents contesting not only political authorities but also super monopolies of massive online platforms and
their peculiar partnerships that they form with diverse governments.

About the author

Zeyno Ustun, Ph.D., is a postdoctoral fellow at the Center for Media at Risk at the University of Pennsylvania.
E-mail: zeyno [dot] ustun [at] asc [dot] upenn [dot] edu

Notes

16. Ibid.
17. Ibid.
24. Ibid.
33. Ibid.
34. Ibid.
References


Editorial history

Received 10 August 2020; revised 18 February 2021; accepted 7 April 2021.

Copyright © 2021, Zeyno Ustun. All Rights Reserved.

Cartographies of digital dissidence: Networked movements, Internet laws, and Internet Ungovernance Forums in Turkey and Brazil
by Zeyno Ustun.
First Monday, volume 26, number 6 (June 2021).
doi: http://dx.doi.org/10.5210/fm.v26i6.11060