Online Activism, Digital Domination, and the Rule of Trolls: Mapping and Theorizing Technological Oppression by Governments

TAMAR MEGIDDO*

The internet and social media have revolutionized activism. However, governments seeking to curb opposition have recently learned to target the very same technologies that empowered activists in the first place. This article challenges the accepted framework for discussing such efforts by governments, centered on surveillance and privacy. It argues, first, that governments' actions should be conceptualized as measures of digital domination. Applying the republican concept of freedom as non-domination, the article suggests that the core harm resulting from such domination is to activists' freedom, not only to their privacy. Since activism is a check on the government, measures undermining the ability to engage in activism also have devastating consequences for the freedom of the citizenry as a whole. Second, the article argues that governments' reliance on digital militias allows them to sidestep the limits of their legitimate authority, therefore posing a grave threat to the rule of law. Finally, the article underscores that governments deploy measures of control beyond surveillance. Rather, they (1) gather information on activists, (2) disrupt communication channels, (3) flood online conversation to drown out the opposition, (4) deploy the state's coercive power based on information gathered, and (5) mobilize digital militias to bully activists online.

* Post-Doctoral Fellow, Minerva Center for the Rule of Law Under Extreme Conditions, University of Haifa. I am grateful to Eyal Benvenisti, Michael Birnhack, Tomer Broude, Hanoch Dagan, Alon Jasper, Sunny Kalev, Roy Kreitner, Noa Kwartaz, Ayelet Sela,

INTRODUCTION

Mainstream media was impressed by the scope and volume of the summer 2019 anti-extradition bill protests in Hong Kong.[1] Hundreds of thousands of protesters filled the streets, challenging Hong Kong's Chief Executive Carrie Lam's intent to introduce a bill permitting extradition to mainland China, which has consequently been shelved by Lam.[2] But this protest was notable not only due to the size of the crowds it drew, but also due to the digitally-informed tactics wielded by its participants. Keenly aware of the watching eye of the state, demonstrators went to great lengths to avoid generating a digital footprint connecting them to the protests and endeavored to create a

Mirjam Streng, Mickey Zar, and Elad Uzan for helpful comments and conversations, as well as to participants of the American Society of International Law Research Forum and workshops and seminars at the Hebrew University of Jerusalem, Tel Aviv University, Bar Ilan University, and University of Haifa. The research was conducted under the auspices of the Minerva Center for the Rule of Law under Extreme Conditions, Faculty of Law and Department of Geography and Environmental Studies, University of Haifa.

1. Austin Ramzy, *Hong Kong March: Vast Protest of Extradition Bill Shows Fear of Eroding Freedoms*, N.Y. TIMES (June 9, 2019), https://www.nytimes.com/2019/06/09/world/asia/hong-kong-extradition-protest.html [https://perma.cc/5GMV-3R4B].

2. Amy Gunia, Hillary Leung & Laignee Barron, *Hong Kong Suspends China Extradition Bill After Protests*, TIME (June 15, 2019), https://time.com/5607678/hong-kong-extradition-bill-suspended [https://perma.cc/5H9E-3YJE].

leaderless protest after leaders of the 2014 Umbrella Revolution were prosecuted and imprisoned.[3] Protesters have thus taken to wearing facial masks and deploying laser guns to avoid detection by facial recognition software. They have resorted to the use of cash only, avoiding even withdrawing money from ATMs in the vicinity of protests. And they have adopted various online anonymity practices by using anonymous and encrypted social networking platforms such as Telegram and switching cell phones and changing SIM cards at every demonstration so as to avoid being tracked.[4] Despite their efforts, certain Telegram group administrators have already been arrested by authorities.[5]

Civil society activism has seen a significant ebb and flow over the past two decades.[6] Technological advancement, and particularly the internet and social media, has revolutionized activism. Thanks to these platforms, activists have been able to connect with others in different urban neighborhoods, cities, and countries and to come together around common causes.[7] By "activists," I am referring to individuals who take part in social or political activity with the goal of affecting change around a defined sphere of life, usually in collaboration with others. This definition is intentionally broad and therefore includes a range of actors from people showing up for a demonstration or occasionally posting messages on social media to individuals who work full-time for a non-profit organization dedicated to a particular cause.

Activists have used the internet and social media in order to

3. Tiffany May, *Hong Kong Umbrella Movement Leaders Are Sentenced to Prison*, N.Y. TIMES (Apr. 23, 2019), https://www.nytimes.com/2019/04/23/world/asia/hong-kong-umbrella-movement.html [https://perma.cc/PJY7-JLND]; *see also* Lokman Tsui, *The Coming Colonization of Hong Kong Cyberspace: Government Responses to the Use of New Technologies by the Umbrella Movement*, 8 CHINA J. COMM. 447 (2015) (describing the Chinese government's catching up with, and even leapfrogging, technological advances to cope with the 2014 Umbrella Revolution).

4. Danny Vincent, *How Apps Power Hong Kong's Leaderless Protests*, BBC NEWS (June 30, 2019), https://www.bbc.com/news/technology-48802125 [https://perma.cc/WV4U-M2U5]; *Hong Kong Protesters Deploy Lights to Demonstrate against "Laser Gun" Arrest*, ABC NEWS (Aug. 8, 2019), https://www.abc.net.au/news/2019-08-08/hong-kong-protesters-use-laser-pointers-as-target-practice/11393692 [https://perma.cc/X2VB-MANE].

5. Vincent, *supra* note 4.

6. *See, e.g.*, Saskia Sassen, *Towards a Sociology of Information Technology*, 50 CURRENT SOC. 365, 380–81 (2002) (discussing how the internet enables a new type of cross-border political activism, once centered in multiple localities yet intensely connected digitally).

7. *Id.* at 379; Jeffrey S. Juris, *Reflections on #Occupy Everywhere*, 39 AM. ETHNOLOGIST 259, 260 (2012).

produce and disseminate information and ideas;[8] generate public awareness; coordinate and mobilize public action;[9] promote their public relations and raise funds;[10] and network with other activists.[11] Social networking platforms have been key in coordinating and mobilizing protest around the world.[12] This has been the case with the anti-austerity protests following the 2008 financial crisis, through the Arab Spring and #Occupy movement,[13] Turkey's pro-democracy demonstrations,[14] and on to the Hong Kong anti-extradition bill protests of the summer of 2019.[15]

Technological developments have also shaped new political subjectivities and helped diffuse new dynamics of activism.[16] Activists created communities and identities that are often transnational in nature, much of whose practice takes place in cyberspace, and which are quite dependent on social media and the internet for their continued persistence.[17] While these activities and

8. Bart Cammaerts, *Social Media and Activism*, *in* THE INTERNATIONAL ENCYCLOPEDIA OF DIGITAL COMMUNICATION AND SOCIETY 1, 7 (Peng Hwa Ang & Robin Mansell eds., 2015) (discussing the spread of the Arab Spring).

9. Alexandra Segerberg & W. Lance Bennett, *Social Media and the Organization of Collective Action*, 14 COMM. REV. 197, 200 (2011) (discussing the use of Twitter as both a networking agent in a transnational protest space and a window into it).

10. Hyunjin Seo, Ji Young Kim & Sung-Un Yang, *Global Activism and New Media*, 35 PUB. REL. REV. 123, 123 (2009).

11. Cammaerts, *supra* note 8, at 7 (explaining the dependency of transnational ties and collective identities on offline performance); Thomas Olesen, *Transnational Publics: New Spaces of Social Movement Activism and the Problem of Global Long-Sightedness*, 53 CURRENT SOC. 419, 420 (2005) (stressing that although transnational publics are mediated and communicated, they are also "very much rooted in real people and places and in face-to-face interactions"); ZEYNEP TUFECKI, TWITTER AND TEAR GAS xxiii (2017).

12. TUFECKI, *supra* note 11.

13. Donatella della Porta & Alice Mattoni, *Pro-Democracy and Anti-Austerity Protests*, *in* SOCIAL MEDIA, POLITICS AND THE STATE 39 (Daniel Trottier & Christian Fuchs eds., 2015); Sara Salem, *The 2011 Egyptian Revolution*, *in* SOCIAL MEDIA, POLITICS AND THE STATE 171, 185 (Daniel Trottier & Christian Fuchs eds., 2015) (but note her conclusion that "while social media has proved to be extremely effective in mobilising protesters, it has been less effective in grassroots organization and political campaigning").

14. TUFECKI, *supra* note 11, at xxvii.

15. Vincent, *supra* note 4.

16. Juris, *supra* note 7, at 260.

17. Cammaerts, *supra* note 8, at 7 ("Increased transnationalization is one of the important ways in which social media are impacting on social movements and protest. Transnational advocacy networks predate the Internet, but networked technologies are providing new opportunities for activists and their organisations to organise at a transnational level. . . . As a result, transnational networks are becoming virtual, more fluid, more

communities have not replaced physical activities in the physical world[18] or activity through other kinds of technology,[19] cyber-based action has become a significant part of activists' practice.[20]

In his 2006 book *The Wealth of Networks*, Yochai Benkler's early account of the internet celebrates the capabilities of online peer production of information and content to replace mass media as democracy's watchdog.[21] At the time of writing, he also posits that it has become increasingly difficult for governments to control the net in order to disrupt such collaboration.[22]

This optimism about the limited capacities of governments to control the net—and with it the promise of the activist networked sphere—has since dissipated.[23] Social media is neither inherently nor

decentralised, more de-institutionalised and more global.").

18. Olesen, *supra* note 11, at 420 ("This does not mean that social space is detached from physical spaces. What it does mean is that local, national and transnational spaces are imbricated in much of today's social movement activism."); Sassen, *supra* note 6, at 380–81 ("Through the Internet, local initiatives become part of a global network of activism without losing the focus on specific local struggles. . . . It enables a new type of cross-border political activism, one centered in multiple localities yet intensely connected digitally.").

19. Segerberg & Bennett, *supra* note 9, at 199 (cautioning against the analytical fallacy of abstracting new social media out of more complex contexts, in the debate about social media and contentious politics).

20. Studying transnational activists' networked communities, Margaret Keck and Kathryn Sikkink describe how activists connect with peers elsewhere and engage in a variety of techniques to "mobilize information strategically to help create new issues and categories and to persuade, pressure and gain leverage, in order to change the behavior of states and international organizations." MARGARET E. KECK & KATHRYN SIKKINK, ACTIVISTS BEYOND BORDERS 2–3 (1998). Keck and Sikkink stress that exchange of information is at the core of such networks although movement of funds, services and personnel are also key: "The ability to generate information quickly and accurately, and deploy it effectively, is their most valuable currency; it is also central to their identity." *Id.* at 9–10; *see also* Peter M. Haas, *Introduction: Epistemic Communities and International Policy Coordination*, 46 INT'L ORG. 1, 32 (1992). Coining the term "epistemic communities," Haas addressed, among others, transnational communities of non-state actors such as members of non-governmental organizations and other members of international institutions. *Id.*

21. Benkler suggests that individuals in a networked public sphere are re-conceptualizing themselves as speakers as opposed to passive listeners. They are thus transforming the production and dissemination of information and analysis from a traditional mass-media structure of one- or few-to-many to one where anyone can be the broadcaster. YOCHAI BENKLER, THE WEALTH OF NETWORKS 216 (2006). "These efforts provide a watchdog, a source of salient observations regarding matters of public concern, and a platform for discussing the alternatives open to a polity." *Id.* at 271–72.

22. *Id.* at 270–71.

23. Ron Deibert, *Cyberspace Under Siege*, 26 J. DEMOCRACY 64 (2015); Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the*

necessarily democracy-increasing.[24] Moreover, "the state has never left the scene" of cyberspace.[25] Activists' reliance on social media leaves a digital footprint[26] that functions as an archive for people, messages, pictures, videos, locations, and additional data.[27] As this article demonstrates, states have learned to utilize activists' reliance on cyberspace in order to curb their activity.[28] In fact, the flow of activists' cyber empowerment has now given way to an ebb of significant government intervention achieved by targeting the very same tools that gave rise to this empowerment in the first place.[29] Concomitantly, activists' ability to serve as democracy's watchdogs has come under significant strain.

Government surveillance has received increasing scholarly attention in the past decades, even giving rise to a new multi-disciplinary scholarly field: surveillance studies.[30] Surveillance studies have dealt as a central theme with the issue of social and political control exercised through the gaze of the state.[31]

Legal scholars, too, have raised concerns about government surveillance.[32] They have highlighted, as a core concern, the grave

Digital Environment, 8 VA. J. L. & TECH. 1, ¶¶ 1–2 (2003); Niva Elkin-Koren & Eldar Haber, *Governance by Proxy: Cyber Challenges to Civil Liberties*, 82 BROOK. L. REV. 105 (2016).

24. MARK ANDREJEVIC, ISPY: SURVEILLANCE AND POWER IN THE INTERACTIVE ERA 190–97 (2007); LAWRENCE LESSIG, CODE 2.0, at 4 (2006).

25. Birnhack & Elkin-Koren, *supra* note 23, ¶¶ 1–2; Elkin-Koren & Haber, *supra* note 23 (both discussing the collaboration between government actors and internet intermediaries in, inter alia, surveillance of citizens).

26. ANDREJEVIC, *supra* note 24, at 2–4.

27. Cammaerts, *supra* note 8, at 6.

28. ANDREJEVIC, *supra* note 24, at 8; Deibert, *supra* note 23, at 64 ("The very technologies that many heralded as 'tools of liberation' four years ago are now being used to stifle dissent and squeeze civil society.").

29. *See generally* TUFECKI, *supra* note 11.

30. David Lyon, Kevin D. Haggerty & Kirstie Ball, *Introducing Surveillance Studies*, *in* ROUTLEDGE HANDBOOK OF SURVEILLANCE STUDIES 1 (Kirstie Ball, Kevin D. Haggerty & David Lyon eds., 2012).

31. *See generally* THEORIZING SURVEILLANCE (David Lyon ed., 2006); *see also* David Lyon, *The Search for Surveillance Theories*, *in* THEORIZING SURVEILLANCE 3, 9–12 (David Lyon ed., 2006) (noting, among others, scholars drawing on Marx, Weber, Simmel, Durkheim, Agamben, and Arendt).

32. As Jack Balkin noted, "[t]he question is not whether we will have a surveillance state in the years to come, but what sort of surveillance state we will have." Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 3–4 (2008). *See generally* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? (2006).

harm to individual privacy that is caused by surveillance.[33] Rather than a narrow interest, theorists have expanded rich, elaborate theories which have "politicized" privacy,[34] underscoring its key importance for the development of the self, for pursuing individual freedom and autonomy, and for one's ability to participate in a political community as an engaged citizen.[35] In other words, privacy theories have viewed it as key for safeguarding individual freedom.

This article explores the practice of governments' use of technological control measures to monitor and curb civil society or political opposition activists. This practice tests the boundaries of the academic literature's present emphasis on surveillance and privacy. As the article shows, governments have deployed a host of technological tools beyond surveillance against actors that they view as posing a threat of political opposition. In addition to governments' information-gathering efforts, the article surveys instances of governments disrupting communications and information flows; flooding the digital environment with disinformation or using large-scale organizing to dominate the online conversation; using information collected through questionable surveillance to mobilize the state's coercive power in order to curb activists; and resorting to harassment and bullying, offline as well as online.[36] Moreover, on many occasions, governments rely on private actors to collect, disrupt or disseminate information, or to harass or threaten activists. Governments are thus able to exceed the formal limits of their authority while maintaining deniability.[37]

Similarly, the harm inflicted on activists as a result of governments' digital control measures extends beyond a violation of their privacy. Activists expressly and deliberately operate in public, with the goal of spreading their message and reaching increasing audiences. Often, activists do not wish to be lost in crowds, and do not

33. Julie Cohen, *Studying Law Studying Surveillance*, 13 SURVEILLANCE & SOC'Y 91, 99 (2014) ("Working together, legal scholars and Surveillance Studies scholars might advance the project of formulating working definitions of privacy interests and harms, and might develop more sophisticated projections of the likely effects of different policy levers that could be brought to bear on systems of surveillance.").

34. Mickey Zar, Plenty to Hide: Resistance to Surveillance as a Political Action (Oct. 29, 2017) (unpublished Ph.D. dissertation, Tel Aviv University) (on file with author) (arguing that "the greatest threat pertaining to privacy is the threat to the feasibility of political action") (translation from Hebrew by author).

35. Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1912–13 (2013); Neil M. Richards, *Privacy and Technology*, 126 HARV. L. REV. 1934, 1946–47 (2013).

36. *See infra* Part I and accompanying text.

37. *See infra* Part II and accompanying text.

seek privacy in their public activities. Rather, they deliberately try to catch others' attention and get them to join them or respond to their claims. The key harm when activists' ability to communicate or demonstrate is curtailed or when they are arrested or attacked is not to their privacy; it is to their freedom.

This article therefore suggests that we ought to reverse lenses. Rather than look at government control measures through the lens of surveillance, we ought to zoom out to recognize the much broader set of tools employed by governments to control their populations and curb opposition. While surveillance is key among these tools, it is not a sole measure. Similarly, rather than discuss political freedom through the lens of privacy, we ought to retain appreciation of privacy's importance in a discussion refocused around individual freedom.

I therefore argue, first, that the technological tools used by governments to curb activists ought to be conceptualized as a set of control measures which pose a threat of government domination. Second, I argue that the harm generated by the deployment of these measures ought to be conceptualized in terms of human freedom, defined in republican theory as non-domination. These measures have devastating consequences not only for the activists targeted, but also for the freedom of the citizenry as a whole. Third, governments' reliance on private actors to circumvent the limits of their authority poses a grave threat to the rule of law. As I show, not only non-democratic but also democratic governments deploy digital control measures against their populations. This is a serious concern, particularly in a period characterized by backsliding democracy, such as the present.

The article offers several contributions. First, it offers a new, fruitful framework to assess the harms associated with government technological empowerment, refocused on the idea of individual freedom. Relying on republican theory, I conceptualize freedom as non-domination and argue that a core risk ensuing from the technological tools employed by governments is the potential of domination that they carry, on top of the recognized harm or chilling effect to specific individual rights such as privacy or speech. Second, the article highlights and problematizes the phenomenon of government-sponsored digital militias and digital mercenaries used to monitor, report or attack activists, and analyzes it as a danger to the rule of law. Scholarly discussion on the collaboration of public and private power has focused on governments' collaboration with

commercial actors, such as internet platforms or tech giants.[38] The phenomenon highlighted by this article reveals that governments are able to circumvent the limits of their legitimate authority, by relying on a large variety of private actors to monitor, report or bully activists, all the while maintaining deniability. This outsourcing of digital oppression brings to light a joining of private and public power that is different from the one more often recognized between government and private commercial actors.[39] Finally, the article offers a novel and more comprehensive categorization of the menu of technological or technologically-induced tools employed by governments against activists. The article highlights types of government action which are often subsumed under the category of surveillance or left outside of the discussion. The new categories proposed are government (1) information gathering, (2) disruption, (3) flooding, (4) policing, and (5) bullying. This new categorization enables a more nuanced analysis of the implications of government action for individual freedom, democratic institutions, and the rule of law.

The first part of the article surveys government digital measures of control and proposes a new categorization. Building on the survey, the second part discusses the harms to individual freedom, democracy and the rule of law, that result from these measures. The article concludes by outlining a future research agenda, developing the themes raised by these practices.

38. *See* Elkin-Koren & Haber, *supra* note 23; Niva Elkin-Koren & Michal S. Gal, *The Chilling of Governance-by-Data on Data Markets*, 86 U. CHI. L. REV. 403 (2019); Balkin, *supra* note 32, at 16–17; Birnhack & Elkin-Koren, *supra* note 23; *see also* K. Sabeel Rahman, *Democracy Against Domination: Contesting Economic Power in Progressive and Neorepublican Political Theory*, 16 CONTEMP. POL. THEORY 41, 41–42 (2017) (noting the concerns that arise from the prospect of government regulation of the market in response to the rise of concentrated private power "in the form of 'too-big-to-fail' financial firms and quasi-monopolies in information and telecom sectors"). This article makes an explicit choice to focus specifically on the concerns arising from government domination through, among others, information gathering. This choice should not be read to deny the surveillance carried out by tech giants over individuals and consumers and the substantial power that such surveillance affords these companies. However, capitalist surveillance is widely discussed in contemporary scholarship. Therefore, the purpose of choosing to focus on governments in this article is to highlight what I believe to be an under-addressed phenomenon: technological domination by governments.

39. This occurs either through the states' regulatory capacity, or by their co-opting such actors. Birnhack & Elkin-Koren, *supra* note 23, at 2.

I. GOVERNMENT CONTROL IN A DIGITAL AGE: A NEW CATEGORIZATION

The internet's original architecture was perceived by many to offer a lawless, stateless zone of liberty, where the long arm of government does not and should not reach.[40] However, despite its liberating potential, cyberspace is not, in fact, completely separate from the physical world and its experiences and constraints.[41] Moreover, governments have continuously worked to close the control gap and the internet is, increasingly, governed by states.[42] The following discussion provides a non-exhaustive survey of many of the technological or technologically-induced tactics that governments have used in order to curb civil society activism or political dissent. The article divides them into five broad categories: Section A discusses information gathering; Section B addresses the disruption of communications and information flows; Section C covers the flooding of online conversation; Section D analyzes the use of policing, by which I refer to the exercise of sovereign coercive powers based on technologically-gathered information; and Section E discusses bullying. Jointly and separately, governments have deployed these measures as a means for significantly jeopardizing activists' ability to coordinate, collaborate and network, to produce and disseminate information, to raise public awareness, and to mobilize public action. In other words, they have targeted the very features that empowered online activism in the first place. While some government interventions aim to constrain activists technologically (e.g., disrupting, flooding), others use offline, physical coercive measures (e.g., policing) whose deployment nonetheless relies heavily on technologically-gathered information.

Nevertheless, it is important to recall that governments have operated to curb dissent prior to the internet. They have gathered information on citizens and dissidents; disrupted protests by physical obstruction or otherwise; used propaganda; and policed and bullied activists, directly or indirectly. However, technology has made a quantitative difference for government power that has had significant qualitative impact in terms of how all-encompassing governments'

40. LESSIG, *supra* note 24, at 4.

41. JULIE E. COHEN, CONFIGURING THE NETWORKED SELF 12–14 (2012) ("The technologies and 'places' that constitute cyberspace have been assimilated into the lives of millions of ordinary people who embrace the Internet as a tool for pursuing their ordinary, real-world ends.").

42. GOLDSMITH & WU, *supra* note 32, at viii. The authors, however, stress that this is not necessarily a bad thing. *Id.*; Elkin-Koren & Haber, *supra* note 23.

reach can be. This is evidenced throughout the survey the article now turns to.

The literature has covered some of the practices I discuss below, primarily in its discussion of government surveillance, or, more recently, "state-sponsored trolling." However, as the new categorization shows, governments have engaged in measures of technological control beyond either surveillance or trolling, so lumping these measures together under only these two categories underplays their significance as standalone measures of control which generate distinct concerns and harms.

A. Gathering Information

Governments' technological information-gathering efforts can be dissected along various organizing themes. The first refers to the actors monitored. For present purposes, the key distinction to make is between the gathering of information on the entire population, key groups (e.g., ethnic minorities), and activists. A second issue is the type of information gathered by governments, which has included biometric data (e.g., fingerprints, face and voice samples, DNA); information regarding communications (including both the content of communications and meta-data); and information regarding movement or location. A third theme refers to the type of actor gathering the information. Here, distinction could be made between information gathering by formal government actors (police, security services), commercial actors regulated or contracted by the state (Internet Service Providers (ISPs), social networking platforms, or even cyberespionage firms hired by the government), and citizens monitoring other citizens. A final key distinction refers to the type of political regime, particularly whether a state is democratic or not.

When it comes to technological information gathering, China is the leading example. It is a pioneer in gathering information on its entire population, while also particularly targeting ethnic minorities and political dissidents. Set to be fully deployed by 2020, China's Social Credit System combines online and offline surveillance tools to monitor and control its citizens,[43] relying not only on government information gathering, but also on commercial actors and other citizens. In line with President Xi Jinping's vision of "internet sovereignty,"[44] beginning shortly after his ascendance to power, Chinese citizens who wished to create social media accounts or use

43. Xiao Qiang, *President Xi's Surveillance State*, 30 J. DEMOCRACY 53, 53 (2019).

44. *Id.* at 54.

internet on their phones were required to register their real names with ISPs[45] or content providers such as social media platforms.[46] These ISPs and content providers are in turn required to surveil their networks, share information with state investigators, and decrease anonymity by requiring real-name registration under the 2016 cybersecurity law.[47] China further required manufacturers and service providers to build surveillance, censorship, or backdoor functionalities into their products, as well as to hand over encryption keys to the government.[48] In addition, China has recruited two million individuals to serve as social media monitors, collecting information on citizens' online behavior.[49] All these enable the government to tightly monitor citizens' online activity, and prevent the use of anonymity or encryption to avoid detection.

China's online surveillance apparatus is complemented by the wide-scale collection of citizens' biometric data, which is also used in order to monitor people's offline movements.[50] Chinese authorities have stored billions of face samples—in addition to millions of voice, fingerprint and DNA samples—and maintain integrated databases where these samples are linked to citizens' national identification numbers.[51] Sample collection is sometimes done without individuals' knowledge or consent, or obtained by compelling individuals to submit to sampling. Such a requirement is not limited to individuals suspected of criminal activity; citizens under no suspicion may likewise be compelled to submit to sampling.[52] These databases are coupled with

45. *Id.*; Deibert, *supra* note 23, at 68.

46. Guobin Yang, *Internet Activism & the Party-State in China*, 143 DAEDALUS 110, 114 (2014).

47. Qiang, *supra* note 43, at 55.

48. Deibert, *supra* note 23, at 67; Yang, *supra* note 46, at 115.

49. *China Employs Two Million Microblog Monitors State Media Say*, BBC NEWS (Oct. 4, 2013), https://www.bbc.com/news/world-asia-china-24396957 [https://perma.cc/C49E-9AKT]; Qiang, *supra* note 43, at 54.

50. Qiang, *supra* note 43, at 56–57.

51. *Id.* at 56–59; *China Collecting "Voice Pattern" Samples to Establish National Biometric Database*, HUM. RTS. WATCH (Oct. 22, 2017), https://www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy [https://perma.cc/ND89-BJ27].

52. Qiang, *supra* note 43, at 58 (explaining that compulsory submission of biometric samples often extends to "not only dissidents and members of the largely Muslim Uyghur ethnic minority, but also migrant workers and even coal miners and property tenants"); *China: Minority Region Collects DNA for Millions*, HUM. RTS. WATCH (Dec. 13, 2017), https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions [https://perma.cc/8EBD-T7SX] (citing concerns that collection of biometric data was done "surreptitiously, under the guise of a free health care program").

widespread coverage of surveillance cameras in public spaces,[53] powered with sophisticated software able to assess crowd density and analyze individual traits such as age, ethnicity, gender and height, as well as characteristics of clothing and vehicles.[54] Advanced facial recognition capacities have allowed authorities to identify specific individuals[55] and pick individuals belonging to the Uighur ethnic minority out of crowds.[56] Nevertheless, despite its much-deserved attention, China is far from the only state employing such technological data-collection instruments.

Several governments have worked to gather information on their populations' communications. Russia requires that telecommunication companies and ISPs to direct copies of all internet communications through governments' servers for inspection and archiving.[57] India listens in on "broadband phone calls, SMS messages and email traffic."[58] Pakistan requires the registration of SIM cards with biometric identification.[59] States' efforts to ensure their ability to monitor communications and their blocking of encrypted communications (to which I return under the next category), indicate that they, too, engage in information gathering. Pakistan bans encryption.[60] And, like China,[61] the United Arab Emirates (UAE) has banned Virtual Private Networks (VPNs) which may assist in avoiding surveillance.[62]

Importantly, not only authoritarian states, but also democratic ones engage in collecting information on their citizens' communications on a wide scale. These efforts generate a standing database of information on all citizens, which can later be "mined" at

53. China's Skynet project, completed in 2017, is the world's largest video surveillance network, including some 176 million cameras at the time with plans of continued growth. Qiang, *supra* note 43, at 57.

54. *Id.* at 56.

55. *Chinese Man Caught by Facial Recognition at Pop Concert*, BBC NEWS (Apr. 13, 2018), https://www.bbc.com/news/world-asia-china-43751276 [https://perma.cc/E5YW-9FKW].

56. Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, N.Y. TIMES (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html [https://perma.cc/2TA4-4PS6].

57. Deibert, *supra* note 23, at 67.

58. *Id.*

59. *Id.* at 68.

60. *Id.* at 67–68.

61. Qiang, *supra* note 43, at 56; Deibert, *supra* note 23, at 67–68.

62. Deibert, *supra* note 23, at 67–68.

will.[63] Edward Snowden's revelations exposed how, under the umbrella of PRISM and other programs, the United States National Security Agency (NSA) and Federal Bureau of Investigation (FBI) compelled Verizon to hand over the meta-data of the phone calls of millions of Americans and gained direct access to the servers of Apple, Google, Facebook, Skype and other tech giants, circumventing encryption and privacy controls.[64] The United Kingdom's "Tempora" program was the British equivalent.[65] In addition, the United Kingdom, the United States, France, Germany, and Sweden are among states reported to place interceptors on fiber-optic submarine internet cables, aimed to harvest data as it travels through them. They have also been known to collaborate and share information on various occasions.[66]

The data collected in such sweeping information-gathering operations may include both content[67] and meta-data.[68] It is important to underscore the significance of meta-data collection.[69] The creation of such comprehensive databases enables not only present or retrospective detection of targeted persons or forms of behavior,[70] but

63. For instance, the FBI and the U.S. Immigration and Customs Enforcement (ICE) are reportedly mining Department of Motor Vehicles (DMV) photo databases in search of undocumented migrants. Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, WASH. POST (July 8, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/ [https://perma.cc/6ELG-37AE].

64. David Lyon, *Surveillance, Snowden, and Big Data*, 1 BIG DATA & SOC'Y. 1, 2 (2014); Zygmunt Bauman et al., *After Snowden: Rethinking the Impact of Surveillance*, 8 INT'L POL. SOC. 121, 123 (2014).

65. Lyon, *supra* note 64, at 2.

66. Bauman et al., *supra* note 64, at 122.

67. Meaning, "recordings of phone calls, text messages, images of web-cams, substance of email messages, entries on Facebook, the history of an Internet user's access to Web sites, and so on." *Id.* at 123.

68. Namely, "data recording the means of creation of transmitted data, the time and date of its creation, its creator, and the location where created." *Id.*

69. Laura Poitras & Glenn Greenwald, *NSA Whistleblower Edward Snowden: "I Don't Want to Live in a Society that Does These Sort of Things"*, GUARDIAN (June 9, 2013), https://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video [https://perma.cc/49MM-26SE].

70. In a recent development in this systematic gathering of information, as of 2019, the United States has added a question to its visa application questionnaire which requires applicants to disclose which social media platforms they have used in the last five years and provide their username or handle (although, graciously, not the password). Sandra E. Garcia, *U.S. Requiring Social Media Information from Visa Applicants*, N.Y. TIMES (June 2, 2019), https://www.nytimes.com/2019/06/02/us/us-visa-application-social-media.html [https://perma.cc/UPN2-CZZC].

also the ability to "mine" the stored information at any future point.[71] Note that authorities have the capacity to monitor not only public information that people publish on social media platforms or other websites,[72] but also private emails and other correspondence,[73] for instance through the use of lawful interception or wiretap of personal communications[74] or even through the use of spyware.[75]

Democratic states also collect wide-scale information on movement and location. In addition to London, which is considered to be one of the most surveilled cities in the world,[76] urban networks of CCTV cameras are proliferating across the U.S., in cities including New York and Baltimore. Chicago, quickly matching up to London, has about 30,000 government-operated cameras,[77] with many private cameras linked to the public system.[78] This has given rise to concerns that the camera network serves to facilitate, entrench and mask the racial bias that has long characterized the local police and includes, importantly for our context, a "long history of monitoring African-American activists that reaches from the Black Panthers to Black Lives Matter."[79] Facial recognition software has been used in several U.S. cities, although some cities, notably San Francisco, have recently banned it.[80] In addition, the U.S. military has recently deployed an

71. Poitras & Greenwald, *supra* note 69.

72. Daniel Trottier, *Vigilantism and Power Users: Police and User-Led Investigation on Social Media*, *in* SOCIAL MEDIA, POLITICS AND THE STATE 209, 215 (Daniel Trottier & Christian Fuchs eds., 2015); ANDREJEVIC, *supra* note 24, at 194–96.

73. Jonathan Cable, *The London G20 Protests in 2009*, *in* SOCIAL MEDIA, POLITICS AND THE STATE 131, 143 (Daniel Trottier & Christian Fuchs eds., 2015) (describing the U.K. Police monitoring "chatrooms, emails, and open sources of information" during the London G20 Protests in 2009).

74. Trottier, *supra* note 72, at 215–16.

75. *Id.* at 216; Doe v. Federal Democratic Republic of Ethiopia, 851 F.3d 7 (D.C. Cir. 2017) (finding Ethiopia immune from suit alleging that it hacked the home computer of an Ethiopian refugee residing in the United States using spyware).

76. Felipe Araujo, *Inside the City That Spies on You*, MEDIUM (Jan. 3, 2019), https://medium.com/s/story/inside-the-city-that-spies-on-you-84b71534309e [https://perma.cc/4FBE-4VF8].

77. Timothy Williams, *Can 30,000 Cameras Help Solve Chicago's Crime Problem?*, N.Y. TIMES (May 26, 2018), https://www.nytimes.com/2018/05/26/us/chicago-police-surveillance.html [https://perma.cc/E7L7-SRDS].

78. Associated Press, *Welcome to Chicago, Most Surveilled City in the World Published*, NBC CHICAGO (Apr. 6, 2010), http://www.nbcchicago.com/news/local/Welcome-to-Chicago-Most-Surveilled-City-in-the-World-89991502.html [https://perma.cc/SP9M-Z4CB].

79. Williams, *supra* note 77.

80. Dave Lee, *San Francisco is First US City to Ban Facial Recognition*, BBC NEWS

experimental wide-area surveillance program in several states,[81] using solar-powered high-altitude balloons which surveil the underlying territory from the stratosphere. These balloons are meant to "provide a persistent surveillance system to locate and deter narcotic trafficking and homeland security threats."[82] This technology is sometimes referred to as "combat TiVo," since the visuals collected and stored enable one to "rewind the tape to see exactly what occurred, and rewind even further to see who was involved and where they came from."[83] While these efforts are aimed to address drug traffickers or terrorists, they create a visual database that covers all human movements in the covered areas which can later be mined for additional purposes.

In addition to conducting surveillance through their various state security organizations, or in collaboration with telecommunication and internet companies, states also rely on a variety of private actors for gathering information.[84] One type of such outsourcing of data-gathering is done by contracting private commercial firms who specialize in cyberespionage.[85] The use of cyberespionage firms allows governments to collect information on particular individuals or groups. The Israeli firm NSO has reportedly sold its sophisticated services to a long list of authoritarian governments, surveilling opposition and civil society activists, and

(May 15, 2019), https://www.bbc.com/news/technology-48276660 [https://perma.cc/RUW6-2T9A].

81. "Up to 25 unmanned solar-powered balloons are being launched from rural South Dakota and drifting 250 miles through an area spanning portions of Minnesota, Iowa, Wisconsin and Missouri, before concluding in central Illinois." Mark Harris, *Pentagon Testing Mass Surveillance Balloons Across the US*, GUARDIAN (Aug. 2, 2019), https://amp.theguardian.com/us-news/2019/aug/02/pentagon-balloons-surveillance-midwest?__twitter_impression=true [https://perma.cc/78EW-PH5M].

82. *Id.*

83. *Id.*

84. *See, e.g.*, Elkin-Koren & Gal, *supra* note 38, at 403, 406 (discussing "governance-by-data," by which governments tap into data collected on citizens by private firms for the purposes of law enforcement); *see also* Trottier, *supra* note 72, at 213. Trottier seems to be particularly worried about one's surveillance by the masses. As he explains, nationalism plays a role in both digital vigilantes' choice of targets and the modes of expression. *Id.* at 220.

85. *See, e.g.*, Human Rights Council, *Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Surveillance and Human Rights*, U.N. Doc. A/HRC/41/35 (May 28, 2019) (expressing grave concern of governments' use of "surveillance software developed, marketed and supported by private companies" which has been shown to lead to "arbitrary detention, sometimes to torture and possibly to extrajudicial killings," and calling for an "immediate moratorium on the global sale and transfer of the tools of the private surveillance industry"); *see also* CARLY NYST & NICK MONACO, STATE SPONSORED TROLLING 28 (2018); Deibert, *supra* note 23, at 69.

collecting their data and meta-data. Citizen Lab, a multidisciplinary laboratory based at the University of Toronto, has been collecting evidence about the expanding global use of NSO's flagship spyware, Pegasus.[86] Particularly, they have traced government use of Pegasus against activists in Mexico,[87] the UAE, Bahrain, and Saudi Arabia.[88] Other global cyberespionage or "Black PR" firms include the Italian Hacking Team, and the British firms Olton and Gamma Group, all linked to authoritarian regimes including Bahrain, the UAE and Egypt.[89]

According to one report, employees of Huawei, the Chinese telecom giant, have helped the oppressive regime of Yoweri Museveni, Uganda's President, to build a surveillance system that enables it to monitor and curb political opposition, including a "Smart City" encompassing thousands of CCTV cameras equipped with facial recognition software, phone tapping and hacking of personal devices. Authorities were therefore able to gain access to opposition leaders' password-protected phones through spyware, access encrypted conversations, and consequently amass and arrest protesters even before a scheduled protest had a chance to begin.[90] In Zambia, Huawei staff reportedly helped authorities to pinpoint the location of opposition bloggers and guide police units deployed to arrest them.[91]

86. CITIZEN LAB, HIDE AND SEEK: TRACKING NSO GROUP'S PEGASUS SPYWARE TO OPERATIONS IN 45 COUNTRIES (2018), https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/ [https://perma.cc/M8K2-SG7W].

87. *Id.* at 9.

88. *Id.* at 10; *Amnesty International Among Targets of NSO-powered Campaign*, AMNESTY INT'L (Aug. 1, 2018), https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/ [https://perma.cc/SBC4-MU3K]. Amnesty International has recently filed a petition with the District Court in Tel Aviv asking that NSO's export license be revoked, citing the use of Pegasus to attack activists in Saudi Arabia, Mexico and the UAE. *Amnesty Supports Legal Action to Stop Chilling Spy Web*, AMNESTY INT'L (May 13, 2019), https://www.amnesty.org/en/latest/news/2019/05/israel-amnesty-legal-action-stop-nso-group-web-of-surveillance/ [https://perma.cc/S85Y-YZ7H].

89. NYST & MONACO, *supra* note 85, at 28; Deibert, *supra* note 23, at 69; MORGAN MARQUIS-BOIRE ET AL., CITIZEN LAB, FOR THEIR EYES ONLY: THE COMMERCIALIZATION OF DIGITAL SPYING (2013), https://citizenlab.ca/storage/finfisher/final/fortheireyesonly.pdf [https://perma.cc/5W4Q-HLWF].

90. Joe Parkinson, Nicholas Bariyo & Josh Chin, *Huawei Technicians Helped African Governments Spy on Political Opponents*, WALL STREET J. (Aug. 15, 2019), https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017?mod=e2tw [https://perma.cc/NW5W-MRCX].

91. *Id.*

A different type of government reliance on private actors for the collection of information is the use of pro-government groups of individuals who are controlled, directed, supported or tolerated by the government to varying degrees. As I elaborate below, these groups engage in multiple types of online activities in addition to information gathering. For these reasons, they have been dubbed "cyber militias,"[92] "digital vigilantes,"[93] or "electronic armies."[94] Some groups are entirely voluntary; others operate as paid contractors for the government, and these differences have important consequences for the legitimacy of their use, as discussed in Part II. User-led or "crowdsourced" surveillance increases governments' surveillance capacities at little or no additional cost.[95] Often, these groups work to collect information on civil society activists. Reports have identified pro-government groups used to monitor network conversations in Turkey and Ecuador, among others.[96] China's anti-terrorist laws encourage "the masses" to report on any "possessing, publishing, printing, or distributing content that contains terrorism, including digital content,"[97] and set out penalties for withholding such information.[98] However, human rights groups assert that the broad definition of terrorism used by China[99] facilitates politically-motivated abuse and persecution of political dissidents and ethnic or religious minorities such as the Uighurs.[100]

As already noted, the information-gathering tools described in

92. NYST & MONACO, *supra* note 85, at 18.

93. Trottier, *supra* note 72, at 213, 218–20.

94. Deibert, *supra* note 23, at 69.

95. Trottier, *supra* note 72, at 213.

96. NYST & MONACO, *supra* note 85, at 18–19.

97. *China: Disclose Details of Terrorism Convictions*, HUM. RTS. WATCH (Mar. 16, 2017), https://www.hrw.org/news/2017/03/16/china-disclose-details-terrorism-convictions [https://perma.cc/6H7V-GZ69].

98. *Id.*

99. As a Human Rights Watch article explains: "Article 3 of the Counterterrorism Law includes in the definition of terrorism, advocacy (ch: zhuzhang) or behavior (ch: xingwei) that elicit panic in society, endanger public security, infringe upon personal and property rights, or threaten state agencies or international organizations through violence, destruction, intimidation, or other means to achieve its political aims. The term advocacy could apply to proposed policy changes or criticism of government policy, or conduct that is within the boundaries of freedom of expression as set out under international human rights law." HUM. RTS. WATCH, *China: Disclose Details of Terrorism Convictions*, *supra* note 97 (internal quotation marks omitted); *see also* HUM. RTS. WATCH, *China Collecting "Voice Pattern" Samples to Establish National Biometric Database*, *supra* note 51.

100. *See* HUM. RTS. WATCH, *China: Disclose Details of Terrorism Convictions*, *supra* note 97.

this section are applicable not only to activists but to all citizens. However, the importance of discussing them in the context of activists derives from the fact that when applied specifically against them, and particularly when coupled with the additional technological control measures described below, they have the power to curb the very operation of civil society. As discussed in Part II in depth, the effect of these measures is not limited to creating a chilling effect on online speech for fear of detection. State surveillance represents more than just a threat of retribution; increasingly, the threat materializes. This is important because such coercion is effective beyond the chilling effects associated with surveillance: activists continue to exhibit resilience in the face of comprehensive surveillance, only to be arrested, prosecuted, stripped of their citizenship, or killed extrajudicially.[101]

B. Disrupting: Blocking the Dissemination of Information & Disrupting Communication Channels

Governments have deployed various digital tools to disrupt activists' ability to disseminate information and to communicate, organize and mobilize publics. Measures range from "wholesale" to "retail" actions, including internet shutdowns; blocking certain social media services at particular times or situations; national firewalls and content filtering systems; takedown of particular websites or users; and distributed denial of service (DDoS) attacks which overload activists' servers and thus disrupt their ability to communicate, disseminate and receive information.

India's August 5, 2019 revocation of the special status of the state of Jammu and Kashmir was coupled with an internet shutdown aimed to quell dissent, a measure it has repeatedly applied in the region previously.[102] Similar shutdowns occurred in Iraq and Iran.[103] Egypt has shut down most of the internet service during the 2011 Tahrir

101. As Tufecki writes with respect to the 2013 military coup in Egypt: "The new military government mowed down more than six hundred protesters in Rabaa Square in Cairo. Sufficiently brutal governments seem not to bother too much with scientific network analysis and the minutiae of secretly surveilled online imprints. Instead, they are often guided by the philosophy 'Shoot at them all, and let terror sort them out.'" TUFECKI, *supra* note 11, at xxviii.

102. Ananya Bhattacharya, *This Is the 51st Internet Shutdown in Jammu and Kashmir in 2019*, QUARTZ INDIA (Aug. 5, 2019), https://qz.com/india/1681333/jammu-and-kashmir-internet-mobile-services-have-been-shut-again/ [https://perma.cc/NNB4-MNS7].

103. Rick Noack, *Iranians Protested. Then, the Internet Was Cut, in a New Global Pattern of Digital Crackdown*, WASH. POST (Nov. 21, 2019), https://www.washingtonpost.com/world/2019/11/21/iranians-protested-then-internet-was-cut-new-global-pattern-digital-crackdown/ [https://perma.cc/ZL4G-HMH2].

protests [104] and Turkey has shut down WhatsApp, Twitter and Facebook during widespread protests in 2016.[105]

With respect to content filtering, the Great Firewall of China is the paradigmatic example.[106] China operates a system of content filtering [107] and blocks thousands of foreign websites.[108] When coupled with a prohibition on using VPNs which allow circumventing censorship mechanisms,[109] and requiring ISPs and content providers to monitor and remove content it deems offensive,[110] China is able to maintain a significant degree of control over the information domestic activists are able to disseminate and to block undesired content quite effectively.

Some countries block the availability of certain web services. For instance, Saudi Arabia has only recently lifted a ban on Voice-over-Internet-Protocol (VoIP) software services which are encrypted and therefore harder to monitor (such as WhatsApp or Skype).[111] Countries can similarly try to ban Tor, a browser that hides user identity and content, but to date only China seems to have succeeded in effectively doing so.[112]

States also take down websites they deem offensive. Among others, China shuts down blogs, microblogs and websites of political dissidents.[113] India blocked Yahoo! Groups.[114] Countries including Bahrain, the UAE, Qatar, Oman, Saudi Arabia, Kuwait, Yemen, Sudan, and Tunisia blocked "websites that provided skeptical views of

104. TUFECKI, *supra* note 11, at xxii.

105. May Bulman, *Facebook, Twitter and Whatsapp Blocked in Turkey After Arrest of Opposition Leaders*, INDEP. (Nov. 4, 2016), http://www.independent.co.uk/news/world/asia/facebook-twitter-whatsapp-turkey-erdogan-blocked-opposition-leaders-arrested-a7396831.html [https://perma.cc/U4BL-ERAP].

106. GOLDSMITH & WU, *supra* note 32, at 92–97.

107. *Id.* at 95–97.

108. Qiang, *supra* note 43, at 55–56.

109. *Id.* at 56; Deibert, *supra* note 23, at 67–68.

110. Qiang, *supra* note 43, at 54.

111. Raf Sanchez, *Saudi Arabia Lifts Ban on Skype and Whatsapp Voice Calls*, TELEGRAPH (Sept. 20, 2017), https://www.telegraph.co.uk/news/2017/09/20/saudi-arabia-lifts-ban-skype-whatsapp-voice-calls/ [https://perma.cc/YZ8B-U3GP].

112. Kari Paul, *Russia Wants to Block Tor, But It Probably Can't*, VICE (Feb. 18, 2015), https://www.vice.com/en_us/article/ypwevy/russia-wants-to-block-tor-but-it-probably-cant [https://perma.cc/9B97-WXUD].

113. Yang, *supra* note 46, at 112–13, 116–17.

114. NYST & MONACO, *supra* note 85, at 8.

Islam, secular and atheist discourse, and sexual content."[115]

Another way for governments to disrupt the dissemination of undesired information or messages is by turning to platforms and asking that certain content or certain accounts be removed or suspended on the ground that they offend the platforms' community rules. Adalah, The Legal Center for Arab Minority Rights in Israel, has recently filed a petition with the Supreme Court, challenging what they describe as an unauthorized and illegal practice of the Israeli government asking social media platforms to remove content. This practice, according to Adalah, has grown five times over the course of 2017 alone, with over 85% of the requests approved by the platforms.[116] Israel's struggle against the pro-Palestine BDS (Boycott, Divestment, Sanctions) movement provides an example of a similar but indirect government action through mobilized publics.[117] The Ministry of Strategic Affairs and Information has recently launched a campaign aimed at recruiting and directing citizens to fight BDS online. The campaign's website identifies social media posts it deems supportive of BDS or rather supportive of Israel against the movement, and calls on the public to report the former posts to the platforms in order to cause their removal and to like or comment positively on the latter posts.[118] It also calls on the public to notify the campaign of posts that may be "of interest" to this effort.[119] Importantly, when a post or an account is reported to a platform as violating its community rules, the platform's response is often to first remove it or suspend the account, and only later allow the account owner to appeal the decision. In the meantime, the owner's ability to communicate through the platform is impeded.

Another way to disrupt activists' ability to communicate or disseminate information is by targeting their ability to access the internet or operate their websites. A DDoS attack achieves this end when "a large number of computers attempts to access one website over and over again in a short amount of time, in the hopes of overwhelming the server, rendering it incapable of responding to

115. *Id*.

116. HCJ 7846/19 Adallah v. State's Attorney Office, Cyber Unit (pending) (Isr.), https://www.adalah.org/uploads/uploads/Cyber_Petition_Final_241119.pdf [https://perma.cc/H369-LNQQ].

117. *See, e.g.*, AdminA 7216/18 Lara Alqasem v. Immigration and Population Authority, para. 17 (2018) (Isr.); AAP 2966/19 Human Rights Watch v. Minister of Interior (Nov. 5, 2019) (Isr.).

118. *Defending Israel Online*, 4IL, https://www.4IL.org.il [https://perma.cc/QTH9-2SSP] (last visited Dec. 10, 2019).

119. *Id.*

legitimate requests."[120] Azerbaijan's Ministry of Transport, Communications, and High Technologies has been linked by digital forensic investigations to a 2017 DDoS attack on independent online media outlets.[121] Similarly, China is reported to have carried out DDoS attacks to throw off the 2014 Hong Kong Umbrella Revolution, toppling the website of a pro-democracy newspaper and an online voting platform run by Hong Kong University.[122]

Finally, another way to disrupt activists' ability to effectively spread their message is to delegitimize and reduce public trust in "all information intermediaries, including journalists, academics, and experts,"[123] thus sowing mistrust and confusion and rendering it difficult for citizens to tell truth from fiction.[124]

Through such measures, governments have targeted activists' reliance on online platforms to spread messages and organize, or to broadcast to, contact or receive support from transnational networks and publics.

C. Flooding: Disseminating Information

Another digital tactic used by governments in their efforts to curb civil society and political opposition has focused on the dissemination of information. I will address two primary types of this practice: circulating disinformation and drowning out oppositional messages, though the two are often deployed in tandem. Zeynep Tufecki dubs this practice "censorship through information glut,"[125] and argues that "censorship in the digital era requires a reframing of the goals of censorship not as a total denial of access, which is difficult to achieve, but as a denial of attention, focus, and credibility."[126] She explains that often the goal is not to convince people of the government narrative, or to comprehensively block oppositional messages, "but to produce resignation, cynicism, and a sense of disempowerment among the people" by flooding audiences with information in order "to dilute

120. MOLLY SAUTER, THE COMING SWARM: DDOS ACTIONS, HACKTIVISM, AND CIVIL DISOBEDIENCE ON THE INTERNET 2 (2014).

121. NYST & MONACO, *supra* note 85, at 24.

122. Tsui, *supra* note 3, at 451.

123. TUFECKI, *supra* note 11, at 231.

124. *Id.*

125. *Id.* at 229.

126. *Id.* at 228.

their attention and focus."[127]

Organized online disinformation campaigns gained notoriety recently with the revelation of Russian intervention in elections across the Western world and particularly the 2016 U.S. Presidential elections and the British Brexit referendum.[128] But disinformation is also widely deployed by governments within their borders as a tool with which to undermine civil society and political opposition. By "disinformation" I am referring to the publication and circulation of false information, separately from instances of hate speech, libelous or threatening messages or "doxing," which I categorize under bullying, below.

Domestic disinformation campaigns are in a sense the twenty-first century incarnation of government propaganda. However, rather than delivered through captured mainstream media channels, disinformation is today disseminated and has its impact amplified through social media.

Disinformation is often coupled with an attempt to "drown-out" oppositional messages by circulating counter-messages on a wide scale in an attempt to dominate the conversations online. Disinformation and drowning-out pro-government networks have reportedly been identified by journalists, researchers and activists in China,[129] Russia,[130] Turkey[131] and the Philippines,[132] as well as in

127. *Id.*

128. Nicholas Thompson & Issie Lapowsky, *How Russian Trolls Used Meme Warfare to Divide America*, WIRED (Dec. 17, 2018), https://www.wired.com/story/russia-ira-propaganda-senate-report/ [https://perma.cc/555V-47E7]; *Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements*, U.S.H.R. PERMANENT SELECT COMM. ON INTELLIGENCE, https://intelligence.house.gov/social-media-content/ [https://perma.cc/AC5Q-TPJS] (last visited Feb. 3, 2020); DIGITAL, CULTURE, MEDIA AND SPORT COMMITTEE, DISINFORMATION AND "FAKE NEWS": FINAL REPORT, 2017-19, HC 1791, § 6 (UK), https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179109.htm [https://perma.cc/6DBC-JZLJ].

129. GOLDSMITH & WU, *supra* note 32, at 97–100; Yang, *supra* note 46, at 116 (explaining that these commentators, known as the "50-cent party," are "employees or volunteers recruited by government agencies to participate anonymously in online discussion and publish views that either support state agendas or help defuse anti-party sentiment").

130. NYST & MONACO, *supra* note 85, at 18.

131. *Id.*

132. JONATHAN CORPUS ONG & JASON VINCENT A. CABAÑAS, ARCHITECTS OF NETWORKED DISINFORMATION: BEHIND THE SCENES OF TROLL ACCOUNTS AND FAKE NEWS PRODUCTION IN THE PHILIPPINES (2018), https://newtontechfordev.com/wp-content/uploads/2018/02/ARCHITECTS-OF-NETWORKED-DISINFORMATION-FULL-REPORT.pdf [https://perma.cc/9AEJ-9M9D].

Israel,[133] and U.S. President Trump has repeatedly retweeted disinformation created or circulated by his supporters.[134] A recent report by the Oxford Internet Institute found evidence of "organised social media manipulation campaigns" in 70 countries.[135]

Government message amplification is done either through networks of human accounts, real or fake, or also with the support of "bots" (software programs designed to mimic human activity on social media) or software such as Tweetdeck which facilitate to a great extent the ability to like, comment and retweet from multiple accounts at once.[136] Often, their task is to reverberate government messages by liking or sharing them on social media or by posting messages supportive of them.[137]

Bots, particularly, have been used to "attack or drown out critics, boost follower numbers, and magnify the messages of political candidates,"[138] as well as to circulate propaganda and disinformation

133. NOAM ROTEM & YUVAL ADAM, THE BIG BOT PROJECT (2019), https://botim.online/static/pdf/big-net.pdf [https://perma.cc/9597-LP7T]; Ronen Bergman, *Twitter Network Uses Fake Accounts to Promote Netanyahu, Israel Watchdog Finds*, N.Y. TIMES (Mar. 31, 2019), https://www.nytimes.com/2019/03/31/world/middleeast/netanyahu-fake-twitter.html [https://perma.cc/HF6U-FS5Y].

134. Elias Groll, *All the President's Trolls*, FOREIGN POL'Y (July 11, 2019), https://foreignpolicy.com/2019/07/11/all-the-presidents-trolls-carpe-donktum-trump/ [https://perma.cc/LKV3-RVXV].

135. SAMANTHA BRADSHAW & PHILIP N. HOWARD, THE GLOBAL DISINFORMATION ORDER: 2019 GLOBAL INVENTORY OF ORGANISED SOCIAL MEDIA MANIPULATION 2 (2019), https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf [https://perma.cc/TRS8-5KJ5].

136. Samuel C. Woolley, *Automating Power: Social Bot Interference in Global Politics*, 21 FIRST MONDAY (Apr. 4, 2016), https://firstmonday.org/ojs/index.php/fm/article/view/6161/5300 [https://perma.cc/K8PJ-R7HW]. Marwick and Lewis define bots as "pieces of software that create content on social media and interact with people." ALICE MARWICK & REBECCA LEWIS, MEDIA MANIPULATION AND DISINFORMATION ONLINE 38 (2017), https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf [https://perma.cc/2ET3-K89Y]; BRADSHAW & HOWARD, *supra* note 135, at 11 (finding evidence of fake accounts, human, bot, and cyborg, being used to spread computational propaganda, including in order to "amplify narratives or drown out political dissent." Use of bots has been evidenced in fifty out of seventy countries surveyed; human-operated fake accounts are reported in sixty out of the seventy countries surveyed); Franziska B. Keller et al., *Political Astroturfing on Twitter: How to Coordinate a Disinformation Campaign*, POL. COMM. 1 (2019).

137. BRADSHAW & HOWARD, *supra* note 135, at 13 (categorizing the messaging and valence strategies of "cyber troops" as including spreading pro-government or pro-party propaganda).

138. NYST & MONACO, *supra* note 85, at 13; MARWICK & LEWIS, *supra* note 136, at 38.

and to manipulate public opinion.[139] Governments used bots to "game" or coopt platforms' algorithms so as to promote their message or drown out a competing message.[140] Government actors reported to have used bots range from Mexico, Turkey, Azerbaijan, Iran, and Morocco, to South Korea, Italy, the U.K., and the U.S.[141] However, Samuel Woolley has suggested that countries with a longer history of democracy "are more likely to only, or exclusively, use bots for social media follower padding," rather than also for silencing the opposition or spreading pro-government messages.[142] The Oxford Internet Institute report also found evidence of government or military-led computational propaganda campaigns in "a small number of democracies," but these seem to be targeted at other countries (such as a USAID creation of a fake social network in Cuba).[143] One example of a domestic use of political bots and amplifying software in a democracy by a government actor is nevertheless provided by South Korea. In the last two election cycles for the country's presidency (2012, 2017), government actors have used such tools to try to sway public opinion in favor of the candidate who was subsequently elected.[144]

Researchers have also identified volunteer, amateur, or professional digital militias, which may be paid or unpaid.[145] Using digital militias or bots serves to conceal the origin of government flooding and make it seem more authentic and widespread by diversifying the character of participating social media accounts disseminating the information, a practice known as "astroturfing". I return to discuss the complexity and implications of pro-government organized networks in Part II.

In addition to astroturfing, another tactic of drowning out is the practice of hashtag "hijacking" where a hashtag associated with a certain political movement is coopted by its opponents by posting messages critical to the original message on a large scale in association

139. Woolley, *supra* note 136.

140. NYST & MONACO, *supra* note 85, at 13.

141. *Id.*

142. Woolley, *supra* note 136.

143. BRADSHAW & HOWARD, *supra* note 135, at 9.

144. Choe Sang-Hun, *South Korean Leader's Ally Convicted of Illegal Pre-Election Influence Campaign*, N.Y. TIMES (Jan. 30, 2019), https://www.nytimes.com/2019/01/30/world/asia/south-korea-president-moon-jae-in.html [https://perma.cc/QH6V-CPRE]; Choe Sang-Hun, *Former South Korean Spy Chief Sentenced for Trying to Sway Election*, N.Y. TIMES (Aug. 30, 2017), https://www.nytimes.com/2017/08/30/world/asia/south-korea-spy-chief-sentenced.html [https://perma.cc/6PS9-S2EP]; Keller et al., *supra* note 136.

145. BRADSHAW & HOWARD, *supra* note 135, at 9.

with the original hashtag.[146] This prevents opposition activists from connecting, communicating, and organizing around the core message.[147]

Finally, both drowning out and disinformation may be achieved effectively through the use of "micro-targeting." Many firms today generate very detailed profiles on users, which facilitate advertising to a very specific focus group. This "social sorting"[148] can be and has been utilized not only for the purposes of commercial advertising, but also for more pernicious ends such as voter suppression. A recent example is the 2016 U.S. presidential elections, where Donald Trump's campaign micro-targeted African-American voters in certain districts with ads aimed to discourage this specific population from going out to vote.[149] These are "dark posts," namely non-public ads shown only to the population segment targeted and not to anyone else.[150]

D. Policing: Mobilizing Sovereign Powers Against Activists

An important feature of the information gathered on activists by government or government-backed surveillance is that it is operationalized, even weaponized, by governments wishing to clamp down on dissent.[151] As United Nations Special Rapporteur on Freedom of Expression David Kaye recently found: "[s]urveillance of specific individuals—often journalists, activists, opposition figures, critics and others exercising their right to freedom of expression – has been shown to lead to arbitrary detention, sometimes to torture and

146. *Id.* at 13; *see also* MARWICK & LEWIS, *supra* note 136, at 35–36 (describing hashtag manipulations in general).

147. Woolley, *supra* note 136.

148. Lyon, Haggerty & Ball, *supra* note 30, at 3.

149. Joel Winston, *How the Trump Campaign Built an Identity Database and Used Facebook Ads to Win the Election*, MEDIUM (Nov. 18, 2016), https://medium.com/startup-grind/how-the-trump-campaign-built-an-identity-database-and-used-facebook-ads-to-win-the-election-4ff7d24269ac [https://perma.cc/3YDL-9TDX]; Joshua Green & Sasha Issenberg, *Inside the Trump Bunker, With Days to Go*, BLOOMBERG (Oct. 27, 2016), https://www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go [https://perma.cc/JS8L-JV4U].

150. Winston, *supra* note 149; Green & Issenberg, *supra* note 149.

151. It is, as Gandy puts it, "[a]ctionable intelligence." Oscar H. Gandy, Jr., *Statistical Surveillance*, *in* ROUTLEDGE HANDBOOK OF SURVEILLANCE STUDIES 125, 125 (Kirstie Ball, Kevin Haggerty & David Lyon eds., 2012); *see also* Lyon, *supra* note 64, at 2.

possibly to extrajudicial killings."[152] Although the two are often linked in practice, this article argues that it is helpful to conceptually distinguish between the exercise of generally legitimate government authority on the basis of digitally-gathered information, and the use of illegitimate and more often privately-executed violence—which I term "bullying." Therefore, under the present category of "policing," I refer only to the former, namely to the exercise of government authority with respect to citizenship and immigration; arrest, detention and criminal prosecution; restrictions on freedom of movement; business licensing; and more.

Under China's surveillance state and particularly its Social Credit System, activists or dissidents who, as a result of their activism, receive a poor social credit score, are denied exit visas and are forbidden to travel outside their region or outside of China.[153] Individuals suspected of terrorism are similarly placed under severe mobility restrictions.[154]

Governments may also deny entry visas to foreign activists in order to prevent them from operating within their borders and collaborating with local activists. Israel's Anti-BDS efforts are an example for this practice. A recent amendment to the Entry into Israel Law forbids the granting of a visa or a residence permit to persons involved with a public call for boycotting Israel.[155] Activists expressing online views supportive of BDS have had their entry visas revoked or their request to renew their residence permit denied, requiring them to leave.[156]

In certain cases, governments even revoked citizenship of

152. Tom Miles, *U.N. Surveillance Expert Urges Global Moratorium on Sale of Spyware*, REUTERS (June 18, 2019), https://www.reuters.com/article/us-socialmedia-un-spyware-idUSKCN1TJ2DV [https://perma.cc/9T95-ZFNH].

153. Don Reisinger, *China Banned 23 Million People From Traveling Last Year for Poor "Social Credit" Scores*, FORTUNE (Feb. 22, 2019), https://fortune.com/2019/02/22/china-social-credit-travel-ban/ [https://perma.cc/PQP3-K5YP]; GOLDSMITH & WU, *supra* note 32, at 87–88.

154. *See* HUM. RTS. WATCH, *China: Disclose Details of Terrorism Convictions*, *supra* note 97.

155. As defined by the Law Preventing Harm to the State of Israel by Means of Boycott, 5771–2011, SH No. 2304 p. 1 (Isr.), https://www.adalah.org/uploads/oldfiles/Public/files/Discriminatory-Laws-Database/English/34-Bill-to-Prohibit-Imposing-Boycott-2011.pdf [https://perma.cc/FL7Q-EYH7].

156. *See, e.g.*, AdminA 7216/18 Alqasem, *supra* note 117; AAP 2966/19 Human Rights Watch, *supra* note 117; Dina Kraft, *Two Leading U.S. Human Rights Activists Refused Entry to Israel, One for BDS Ties*, HAARETZ (May 3, 2018), https://www.haaretz.com/israel-news/.premium-two-leading-u-s-human-rights-activists-deported-from-israel-1.6052515 [https://perma.cc/M46R-4LKM].

activists due to their online activities. In 2015, Bahrain revoked the citizenships of Ali al-Dairi, the founder of the news outlet *Bahrain Mirror*, and Ali Abdulemam, a popular activist blogger.[157] Human Rights Watch reports that this practice is widespread among Gulf Countries.[158]

Governments also arrest, prosecute, and imprison activists for their online activity.[159] The discussion returns to enforced disappearances and extrajudicial killings under the category of bullying. Here, the focus is on the use of the formal legal system.[160] In China, a 2013 ruling by the Supreme People's Court and Supreme People's Protectorate upheld rules setting prison terms for social media users who spread "defamatory rumors."[161] In Russia, Yegor Zhukov, a 21-year old student and vlogger was recently convicted and sentenced to three years' probation for his political posts, in which he commented, for instance, that "madmen" like Russia's President Vladimir Putin view political power as an end rather than a means. One condition for his probation is that he is banned from posting on the internet.[162] In Bangladesh, Dilip Roy, a 22-year old student, was arrested and prosecuted in August 2016, following his criticism on Facebook of the Prime Minister and his party's support of a new coal power plant.[163] In Turkey, Barbaros Şansal, an LGBT activist, was arrested and prosecuted in 2017 for comments made in a video and two tweets, which were deemed to incite the public to "hatred or hostility."[164] Similar incidents were reported in Saudi Arabia, Bahrain, and the UAE,[165] as well as in Cambodia, Egypt, Kenya, and

157. NYST & MONACO, *supra* note 85, at 26.

158. *Arab Gulf States: Assault on Online Activists*, HUM. RTS. WATCH (July 12, 2017), https://www.refworld.org/docid/59661cf64.html [https://perma.cc/YP9R-XFRV].

159. Yang, *supra* note 46, at 112–13, 117; GOLDSMITH & WU, *supra* note 32, at 87–88.

160. AMNESTY INT'L, HUMAN RIGHTS DEFENDERS UNDER THREAT 11 (2017).

161. Qiang, *supra* note 43, at 54; *China Issues New Internet Rules That Include Jail Time*, BBC NEWS (Sept. 9, 2013), https://www.bbc.com/news/world-asia-china-23990674 [https://perma.cc/D2XB-V7RA].

162. Masha Gessen, *A Powerful Statement of Resistance from a College Student on Trial in Moscow*, NEW YORKER (Dec. 7, 2019), https://www.newyorker.com/news/our-columnists/a-powerful-statement-of-resistance-from-a-college-student-on-trial-in-moscow [https://perma.cc/ZH4Y-4RM7].

163. AMNESTY INT'L, *supra* note 160, at 13.

164. *Id.* at 37.

165. *See* HUM. RTS. WATCH, *Arab Gulf States: Assault on Online Activists*, *supra* note 158.

Rwanda.[166]

Governments may also engage in preventive detention, relying on predictive algorithms in order to uproot what they view as oppositional activism before it even begins. [167] In China, counterterrorism laws allow for pre-police investigation arrest of individuals suspected of terrorism due to online activity, effectively placing individuals under administrative detention and withholding their right to an attorney.[168]

Finally, another item in governments' tool kit is their licensing authority. In the Philippines, Rappler, an online news website critical of Rodrigo Duterte's government, had its business license revoked in January 2018 by the Securities and Exchange Commission.[169]

As this survey shows, governments have resorted to using a range of coercive powers to curb activists. While this practice is more frequently exercised by non-democratic governments, this is not exclusively the case.

E. Bullying: Harassment, Threats and Violence

Making use of the information gathered through the questionable practices described above, some governments have resorted to violence against activists. [170] The murder of Saudi journalist Jamal Khashoggi in the Saudi consulate in Istanbul serves as a somber reminder of this fact. Digital forensics activists have revealed the spyware trail leading up to his murder, showing that the phone of Omar Abdulaziz, Khashoggi's colleague and himself a Saudi dissident living in Canada, was infected with Pegasus spyware which granted his attackers full access to his communications with Khashoggi in the run-up to his murder.[171]

166. FREEDOM HOUSE, FREEDOM ON THE NET 4–5 (2018), https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf [https://perma.cc/RE7G-C9MJ].

167. Qiang, *supra* note 43, at 58.

168. *See* HUM. RTS. WATCH, *China: Disclose Details of Terrorism Convictions*, *supra* note 97.

169. NYST & MONACO, *supra* note 85, at 33.

170. CITIZEN LAB, *supra* note 86, at 3.

171. Max Boot, *An Israeli Tech Firm is Selling Spy Software to Dictators, Betraying the Country's Ideals*, WASH. POST (Dec. 5, 2018), https://www.washingtonpost.com/opinions/2018/12/05/israel-is-selling-spy-software-dictators-betraying-its-own-ideals/ [https://perma.cc/PGS3-NNAF]; Hagar Shezaf, *Revealed: Israel's Cyber-spy Industry Aids World Dictators Hunt Dissidents and Gays*, HAARETZ (Oct. 19, 2018), https://search.proquest.com/

In Pakistan, bloggers Asim Saeed, Ahmed Raza Naseer, and Waqas Goraya, and online activists Salman Haider and Sammar Abbas were subject to enforced disappearance by security forces. The first four were reunited with their families after more than three weeks, but Abbas remains missing, and his fate unknown. The five used social media to express and disseminate views critical to the Pakistani religious and military establishment and to support human rights.[172]

As indicated above, governments increasingly rely on non-official networks of supporters to gather or spread information or to disrupt activists' communication channels. Such networks have also been mobilized in some circumstances to bully activists online.[173] "Trolling" is an understudied phenomenon which refers, generally speaking, to online activity aimed to create disruption or conflict.[174] The phenomenon on which this article focuses is the government-coordinated activity of groups of online actors, which has been referred to by scholars and activists as "state-sponsored trolling." However, for present purposes, the concept of trolling seems at once under-inclusive and over-inclusive. It is under-inclusive because the discussion in this article of pro-government online actors includes their efforts to gather information, not just bully or disrupt communications. It is over-inclusive because it carries a (negative) moral judgement applied to the entirety of such groups' online activity. Yet, as discussed at greater length below, it is not necessarily the case that the organized, wide-scale reverberation of government messages carried out by supporters of a government is illegitimate when done entirely voluntarily. Therefore, the following discussion of bullying is limited to violent online (or occasionally offline) attacks by organized networks which are orchestrated by government actors who either explicitly identify targets for attack or use dog-whistle cues to set off their supporters against activists.

Several governments have declared publicly, and for others it has been revealed, that they support or operate organized online groups. Sometimes these are volunteer groups, such as the Russian

docview/2122329646/citation/6C1DE70B574B450CPQ/1 [https://perma.cc/8UB6-KCNU]; David D. Kirkpatrick, *Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says*, N.Y. TIMES (Dec. 2, 2018), https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html [https://perma.cc/HS53-F5ST].

172. AMNESTY INT'L, *supra* note 160, at 11.

173. NYST & MONACO, *supra* note 85, at 1.

174. *But see* Katy Pearce, *Two Can Play at That Game: Social Media Opportunities in Azerbaijan for Government and Opposition*, 22 DEMOKRATIZATSIYA 39, 55 (2014) (reviewing various definitions of "trolls").

youth group Nashi or the Azeri youth group Ireli.[175] At other times, they are paid for by governments and deployed by commercial firms.[176] Ecuador's former president Rafael Correa is notorious for his vocal support and encouragement of trolls.[177] In 2015, he launched a website, Somos+ ("We are+"), created with the express purpose of countering anti-government critics online, and responding to posts and memes opposing or disparaging him on social media. The site gained as many as 72,000 registered users.[178] He also hired a private company to operate a troll center to attack and monitor dissidents.[179] Similarly, Venezuela's government has explicitly announced its intent to train "digital guerillas."[180] Telegram channels openly operated by the Venezuelan Ministry of Communications have "disseminated hashtags, memes, and content to be used in the state's trolling attacks on targets."[181]

States may sometimes encourage trolling in more nuanced ways, using dog-whistling to signal to supporters of selected targets without expressly calling for attacks. In this manner, they are able to outsource harassment campaigns to seemingly private actors while ensuring that this activity remains at arm's length from them, affording them at once the power and benefit of the attack as well as deniability.[182]

Online bullying often takes the form of hate speech and misogynistic language, rape and death threats, libelous or false accusations (often of treason or collusion with foreign agents), doctored images or videos, or offensive memes which are then circulated broadly in a coordinated manner.[183] These attacks may last days and flood the targeted activist's account with hundreds or

175. NYST & MONACO, *supra* note 85, at 18.

176. *Id.* at 25; Rebeca Morla, *Correa's Social-Media Troll Center Exposed in Quito*, PANAM POST (Mar. 25, 2015), https://panampost.com/rebeca-morla/2015/03/25/correas-social-media-troll-center-exposed-in-quito/ [https://perma.cc/GWW3-FHUY].

177. Soraya Constante, *Correa Recibe de su Propia Medicina en las Redes Sociales*, EL PAÍS (Feb. 4, 2015), https://elpais.com/internacional/2015/02/04/actualidad/1423076927_196128.html [https://perma.cc/3GSS-PPMC].

178. *Id.*

179. NYST & MONACO, *supra* note 85, at 14, 19.

180. *Id.* at 42.

181. *Id.* at 43.

182. *Id.* at 19.

183. *Id.* at 1, 12–13; *see also* Katy E. Pearce, *Democratizing Kompromat: The Affordances of Social Media for State-Sponsored Harassment*, 18 INFO. COMM. & SOC'Y 1158, 1168 (2015) (discussing the public release of secretly filmed and fake "sex-tapes" of female investigative journalists in Azerbaijan).

thousands of messages, a scale which may be achieved by using bots.[184] Bullying may further include "doxing," or the publishing of a person's personal details online (including their home address, work details, phone number, financial or medical information, details about their family, and more). Doxing can create a real or perceived threat of physical violence, and it is often accompanied with such threats.[185] Bullying often expresses nationalist or xenophobic sentiment in both the choice of targets and modes of expression.[186]

***

As this survey has shown, in addition to surveillance, which has received much scholarly attention, and trolling, which academics have only begun to study, a whole host of government actions use technology to monitor, silence, or undermine civil society and political opposition. Expanding academic discussion beyond these two concepts is necessary in order to represent the variance of oppressive methods deployed by governments and their total impact.

It is worth noticing the myriad ways in which governments rely on private actors, not only in their exercise of formal authority, but also, when the means of law do not suit them, by outsourcing information gathering, disruption and dissemination, as well as outright violence, to online mobs. As discussed in Part II, this makes public use of private power a threat to the rule of law, rather than merely an instance of insufficiently controlled rule by law.

Finally, governments' digital tools are often introduced through "pilot" programs applied to marginal groups, such as foreigners, immigrants, or minorities, or experimented with in the name of fighting crime or protecting national security.[187] Subsequently expanding the scope of such measures to increasingly large populations often occurs by way of mission creep,[188] whether publicly acknowledged or not.[189] Such practices further proliferate across countries and regions.[190]

184. NYST & MONACO, *supra* note 85, at 1.

185. Trottier, *supra* note 72, at 213, 218–20.

186. *Id.*

187. *See* ANDREJEVIC, *supra* note 24, at 209–10, for a discussion of public habituation to surveillance. For a recent example whose development we will have to follow, see Harris, *supra* note 81.

188. Trottier, *supra* note 72, at 211–12.

189. *See also* Bauman et al., *supra* note 64, at 125–26 (discussing the slippage between "foreigner" and "domestic").

190. Qiang, *supra* note 43, at 62; Deibert, *supra* note 23, at 71–73.

II. REVERSING LENSES

A. Beyond Surveillance and Privacy

Government surveillance of citizens has received much scholarly attention over the past decades, and particularly with the advancement of information technologies, giving rise to a new scholarly field: surveillance studies.[191] Surveillance has been broadly defined as "any systematic, routine, and focused attention to personal details for a given purpose."[192] Scholars have studied various forms of surveillance, including peer-to-peer (or lateral) surveillance,[193] capitalist surveillance (as a key basis of companies' business models),[194] and state surveillance of citizens, for instance, in the context of counter-terrorism[195] or crime prevention.[196] While surveillance is not a new phenomenon, scholars stress that its intense proliferation in the late twentieth and early twenty-first century has rendered it "the dominant organizing practice of late modernity."[197]

Surveillance studies have dealt as a central theme with the use of surveillance as a mode of exercising social and political control. This has been paradigmatically conceptualized around the powerful idea of a "panopticon," proposed by Jeremy Bentham and elaborated by Michel Foucault.[198] But scholars have also explored a range of

191. *See, e.g.*, Simon G. Davies, *Surveying Surveillance*, *in* COMPUTERS, SURVEILLANCE, AND PRIVACY 260 (David Lyon & Elia Zureik eds., 1996).

192. Lyon, Haggerty & Ball, *supra* note 30, at 1–2.

193. ANDREJEVIC, *supra* note 24, at 212–40.

194. Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75 (2015); SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM (2019).

195. Bryce Clayton Newell, *Technopolicing, Surveillance, and Citizen Oversight: A Neorepublican Theory of Liberty and Information Control*, 31 GOV'T INFO. Q. 421, 425–26 (2014).

196. Trottier, *supra* note 72.

197. Lyon, Haggerty & Ball, *supra* note 30, at 1.

198. MICHEL FOUCAULT, DISCIPLINE AND PUNISH 195–228 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1977); *see, e.g.*, Bart Simon, *The Return of Panopticism*, 3 SURVEILLANCE & SOC'Y 1, 2–4 (2005). The Panopticon's origin is an architectural design of a prison featuring a ring-shaped building constructed around a central tower, which provides the occupants of the tower with a complete view of all activity in the building. The building's outer ring is divided into holding cells. This design is meant to ensure the control of the supervisors in the tower over prisoners held in the cells. For Foucault, this design is the image of total vision and control, mirrored by total helplessness and consequent self-policing on the part of the prisoners.

additional perspectives to account for the ways in which the surveilling gaze disciplines and controls social subjects.[199] Scholars have given attention to surveillance conducted through information technology ("dataveillance")[200] and addressed the all-encompassing coverage of the "surveillant assemblage," made up of the combination of various surveillance techniques and surveilling institutions across social contexts.[201]

However, by focusing on the particular practice of surveillance, scholars have devoted resources primarily to the gaze, the paying of attention, the collection, storing, and also the analysis of data.[202] The additional technological control measures discussed in Part I—disrupting communication channels, flooding social media with government-sponsored information or disinformation, mobilization the state's coercive power, or bullying—remain outside the purview of surveillance studies. Although practices that fall under these additional categories are occasionally discussed by surveillance scholars, they remain ancillary to the field's core interest. Therefore, this article argues that we should pay attention to the whole host of government control measures and consider them collectively as a set of tools used by governments to curb activists. Paraphrasing on Kevin Haggerty and Richard Ericson's "surveillant assemblage," the argument here proposes to explore the assemblage of control, of which surveillance is only one facet.[203]

The scholarship's attention to the practice of surveillance has been mirrored by a tendency to highlight certain kinds of effects that follow from it. Understanding surveillance as social control or social ordering, [204] the literature has emphasized particularly how surveillance leads to self-discipline and "soul-training,"[205] affected through "chilling effects" for the person watched.[206] Knowing that they are watched, filmed or recorded, individuals tend to self-censor,

199. *See* Lyon, *supra* note 31, at 9–12 (noting, among others, scholars drawing on Marx, Weber, Simmel, Durkheim, Agamben, and Arendt). *See generally* THEORIZING SURVEILLANCE, *supra* note 31.

200. Roger Clarke, *Information Technology and Dataveillance*, 31 COMM. ACM 498 (1988).

201. Kevin D. Haggerty & Richard V. Ericson, *The New Politics of Surveillance and Visibility*, *in* THE NEW POLITICS OF SURVEILLANCE AND VISIBILITY 3, 4 (2007).

202. *See* Lyon, *supra* note 64.

203. Haggerty & Ericson, *supra* note 201.

204. Davies, *supra* note 191, at 2.

205. *Id.* at 4–5.

206. *Id.* at 5.

and thereafter they become moved to ingratiate the person in power, to express those positions favorable to her, or act in manner that will curry her favor.[207]

However, this emphasis on self-discipline is challenged when discussing activists' resistance to surveillance-based control.[208] Activists around the world have exhibited incredible persistence and resilience in the face of overwhelming surveillance and oppression. As the story with which this article begins demonstrates, even in the face of the mighty technological prowess of the Chinese government, Hong Kongers insist on speaking out and protesting, and continue to seek new and creative ways to unburden themselves from the reach of technological as well as political domination.[209] Bart Simon writes that ". . . structuring the seeing/being seen relationship alone is not enough to effect social control."[210] And indeed, activists are often able (or at least make a genuine effort) to fight off the disciplinary effects of surveillance.[211] Therefore, although chilling effects and self-discipline are clearly important, they are not wholly deterministic or sufficient to establish control.[212]

The concept of privacy has received a particularly central role in scholarly efforts to conceptualize the harms of surveillance. As Simon Davies writes: "There exists a very important relationship between privacy and surveillance. . . . [P]rivacy and surveillance are opposing poles of the same magnet. Privacy protection is a defense against surveillance. Surveillance is an intrusion into privacy."[213] Julie Cohen embraces this coupling, highlighting the importance of framing the effects of surveillance "in ways in which legal systems can

207. *Id.*

208. *See, e.g.*, Zar, *supra* note 34 (describing digital resistance to surveillance as a form of political action).

209. As Tufecki writes: "Rising in opposition to crumbling, stifling regimes that tried to control the public discourse, activists were able to overcome censorship, coordinate protests, organize logistics, and spread humor and dissent with an ease that would have seemed miraculous to earlier generations." TUFECKI, *supra* note 11, at xxii.

210. Davies, *supra* note 191, at 7.

211. Tufecki writes: "In fact, as I stood in Gezi Park, tweeting from a phone tied by law to my unique citizenship ID number in Turkey, I knew that the government surely had a list of every protester who showed up at the park with a phone. Despite this fact, once protests broke out on a large scale, the threat of surveillance deterred few people, partly because they felt protected by the scale of the massive protest." TUFECKI, *supra* note 11, at xxvii.

212. As Davies points out, "[d]espite the various structuralist readings of Discipline and Punish that deny agency to subjects (Lyon 1994) the story of the inmate is ultimately not a deterministic story, but rather a voluntaristic one." Davies, *supra* note 191, at 7.

213. *Id.* at 268.

respond" to them.[214] She warns of ineffectual "talk of power, power everywhere,"[215] and underscores that privacy and data protection remain salient legal categories in response to surveillance.[216]

While Cohen is justified in her insistence on speaking about surveillance in a "legal language" in order to facilitate legal action in response, it is nevertheless crucial to reconsider our exclusive commitment to the legal categories she champions. As this part shows, even on the rich account of privacy that Cohen proposes (and to which the discussion will soon return), these categories are unable to account for the full harm of the entire panoply of government control measures surveyed above. Therefore, the legal practicality of these categories must not be allowed to limit our recognition of what is at stake. I argue that the human interest threatened by technologically-bolstered government power is not only privacy, but ultimately human freedom, and it is freedom that needs to occupy center stage in the scholarly conversation.

Cyberspace's propensity to be used to perfect control and extinguish liberty has not been overlooked by lawyers.[217] Lawrence Lessig's *Code* expresses grave concern about the collaboration between public and private power. Warning in 2006 of a cyberspace completely controlled by not only the government,[218] but also by government together with commerce, Lessig writes of "[a] future of control in large part exercised by technologies of commerce, backed by the rule of law (or at least what's left of the rule of law)."[219] In a 2013 essay, Jack Balkin opines that "[t]he question is not whether we will have a surveillance state in the years to come, but what sort of surveillance state we will have."[220] He concludes that one of the dangers of such a state is private power and public-private cooperation, since "government has increasing incentives to rely on private enterprise to collect and generate information for it."[221] Jack

214. Cohen, *supra* note 33, at 98.

215. *Id.* Cohen concludes this argument by suggesting that "[w]orking together, legal scholars and Surveillance Studies scholars might advance the project of formulating working definitions of privacy interests and harms, and might develop more sophisticated projections of the likely effects of different policy levers that could be brought to bear on systems of surveillance." *Id.* at 99. This article seeks to challenge this goal as too narrow.

216. *Id.* at 98.

217. LESSIG, *supra* note 24, at 4.

218. In his assessment, the future is not totalitarian control by the state, but rather the interwoven control of state and commerce. *Id.* at xv.

219. *Id.*

220. Balkin, *supra* note 32, at 3–4.

221. *Id.* at 16–17.

Goldsmith and Tim Wu's *Who Governs the Internet?* notes the renewed control of governments over the internet following its hyper-libertarian early days but suggests that this is not necessarily a bad thing.[222] They indicate that government control through the internet operates through various intermediaries and techniques, including not only control of internet transport but also the targeting of individuals (i.e., arrest and prosecution).[223]

Nevertheless, the main lens through which legal scholarship has conceptualized the harm created by technologically-bolstered control measures (and particularly, surveillance) has been that of privacy.[224] Specifically, privacy has served as a key theoretical lens for discussing concerns associated with the risks to liberty that arise from surveillance. Julie Cohen's theory of privacy conceptualizes it as a prerequisite for human freedom. When one's privacy is diminished, so is her capacity for critical subjectivity and her ability to exercise engaged citizenship; in other words, without privacy there is no human freedom. Moreover, a severely undermined right to privacy also jeopardizes democratic self-government.[225] Cohen's theory of privacy builds on the concept of a "situated" self.[226] She stresses that self-development occurs in a social context, in performative experiences and in relationships with others.[227] Building on Amartya Sen and Martha Nussbaum's[228] "capabilities approach,"[229] she defines

222. GOLDSMITH & WU, *supra* note 32, at viii, 72.

223. *Id.* at 72–81 (identifying control for legitimate aims: enforcement of laws against hate speech, copyright protection, drugs, etc.).

224. Neil Richards has argued that other than a vague idea that surveillance is wrong, an account of what exactly is harmful about government surveillance, and why that is so, is lacking. He suggests that surveillance is harmful for two reasons. First, it can chill the exercise of civil liberties, which requires a degree of "intellectual privacy." Second, surveillance offers power to the watcher over the watched. Richards, *supra* note 35, at 1935. When discussing the power imbalance between the watcher and the watched, Richards points out that it creates a "risk of a variety of harms, such as discrimination, coercion, and the threat of selective enforcement, where critics of the government can be prosecuted or blackmailed for wrongdoing unrelated to the purpose of the surveillance." *Id.* at 1935, 1952–58. *But cf.* Elkin-Koren & Haber, *supra* note 23.

225. Cohen, *supra* note 35, at 1912–13; *see also* Zar, *supra* note 34, at 35 (underscoring the connections between privacy's core importance of development of one's identity and her ability to perform as an engaged citizen in a democracy, and between the personal/individual and public/social aspects of privacy).

226. COHEN, *supra* note 41, at 5–7.

227. *Id.* at 128–31.

228. Sen and Nussbaum ally themselves with Rawlsian liberalism. Martha C. Nussbaum, *Public Philosophy and International Feminism*, 108 ETHICS 762, 771 (1998).

229. *Id.* at 768–70; AMARTYA SEN, DEVELOPMENT AS FREEDOM 290–95 (1999).

freedom "in terms of the development of affirmative capabilities for flourishing,"[230] and insists that any legal framework discussing privacy must attend to the social and cultural conditions that make human flourishing possible.[231] Along the same lines, Neil Richards argues that the harm to one's "intellectual privacy" is a key effect of surveillance. He defines intellectual privacy as a core subset of privacy, which is necessary for individuals to be able to make up their own mind, encompassing the freedoms of thought, belief, and speech, as well as association and assembly. He posits that intellectual privacy is required for the survival of a free society.[232]

Privacy theorist Helen Nissenbaum is a pioneer in recognizing that monitoring of individuals in public may nevertheless implicate their privacy and carries distinct harms.[233] As she explains, privacy is often considered to cover a person's "intimate, private realms" and philosophical and legal theories of privacy "suffer a theoretical blind spot when it comes to privacy in public."[234] Prior to the rise of information technologies, Nissenbaum reminds us, a person could reasonably expect to be lost in the crowd, so to speak, and so gain a large degree of privacy even in public.[235] Today, "information that was once scattered and transient may now be ordered, systematized and made permanent."[236] Moreover, information can easily now be merged, compared, and communicated across networks.[237] Nissenbaum argues convincingly that a person's privacy is violated when private information disclosed in a particular context is transported into a different social context, in disregard of the conditions under which the original disclosure was made.[238] She further suggests that aggregation of data from multiple sources and the creation of profiles provide descriptive access to an individual that,

230. COHEN, *supra* note 41, at 22.

231. *Id.* at 5–7.

232. Richards, *supra* note 35, at 1946–47.

233. Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 L. & PHIL. 559 (1998); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 101 (2004).

234. Nissenbaum, *Protecting Privacy in an Information Age*, *supra* note 233, at 564.

235. *Id.* at 576.

236. *Id.* at 577.

237. *Id.*

238. *Id.* at 581–86; Nissenbaum, *Privacy as Contextual Integrity*, *supra* note 233, at 118–25 (proposing that in different social contexts, privacy entails different rules of appropriateness and distribution which govern when and under which circumstances information provided may be disclosed). *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT (2010).

too, violates her privacy.[239] Daniel Solove proposes a corresponding refutation of the "no privacy in public" argument, denouncing the "secrecy paradigm" which is at its foundation, and stressing the great power that watching provides to the watcher over the person watched.[240]

Nissenbaum and Solove propose compelling accounts for the legitimate expectation of privacy even in public under certain circumstances, but their theories do not account for the harm to activists resulting from surveillance, let alone other control measures. Activists deliberately operate in public, disseminating information in the public sphere of cyberspace with the intent of spreading out the message to others so as to convince them, collaborate, or form alliances. Often, these are not individuals who wish to be lost in the crowd or who expect privacy in their public activity. They set no rules of dissemination on the information they publish; or rather, their rule is: pass it on. They wish to be seen. Consequently, it is not the privacy of these activists that is harmed as a result of government control measures. As I argue below, it is their freedom.

Privacy scholarship dedicates particular attention to the issue of control of information. Under the approach of "Privacy as Control," privacy is understood as the right to control one's information and determine the extent to which and the conditions under which it is communicated to others.[241] Within this conception, too, the harm to activists as a result of surveillance cannot easily be understood as a harm to their privacy: the conditions they set for the information they publish normally allow for its widespread dissemination, often with their knowledge and acceptance that it will also reach government actors.[242] Nevertheless, as argued under the next section, activists do suffer harm as a result of government surveillance and the use of other digital control measures.

Moreover, many of the government control measures discussed in Part I are not restricted to information about people. Disrupting the ability to communicate and organize, limiting activists' liberty of movement through travel bans, arrest and prosecution, rendering them

239. Nissenbaum, *Protecting Privacy in an Information Age*, *supra* note 233, at 586–90.

240. DANIEL J. SOLOVE, NOTHING TO HIDE 178–81 (2011).

241. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967). For a defense of "Privacy as Control," see MICHAEL D. BIRNHACK, מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה [PRIVATE SPACE: THE RIGHT TO PRIVACY, LAW AND TECHNOLOGY] 89–136 (2011); Michael D. Birnhack, *A Quest for a Theory of Privacy: Context and Control*, 51 JURIMETRICS 447 (2011).

242. However, "doxing" seems to be a clear exception to this rule. The above discussion refers to assumed publicity of information disseminated by activists and the fact of their public activity, not their or their families' personal information.

without the protection of a state of nationality by revoking their citizenship and more are not harms to one's control over one's information. They are harms to their ability to stimulate, organize and carry out political action. They are harms to their freedom.

Andrew Roberts criticizes privacy and surveillance scholars for under-appreciating the role of power:

> "Surveillance scholars and sociologists have recognized that surveillance provides the observer with power over the observed. . . . Privacy scholars have taken up this idea and suggested that we should think about the harm to which the loss of informational privacy gives rise in terms of the power that others acquire over us as a consequence. But those who have acknowledged the relationship between surveillance, the loss of privacy and the acquisition of power appear to have recognized neither the importance of participation in political decision making as means for controlling power nor the role of privacy in facilitating such participation."[243]

Roberts explains this oversight as one anchored in liberal versus republican theoretical commitments.[244] Liberal and republican theories and their applications to the present context are discussed in the next section. Roberts's remedy to such shortcomings is to offer a republican theory of privacy, arguing that privacy may serve as a shield for individuals against the threat of domination.[245] Roberts explains that the loss of privacy that we suffer when others watch us or obtain information about us is harmful "to the extent that it provides others with the power to interfere in our decisions that we do not control. . . . This harm arises whether or not we are aware" of being watched.[246] Furthermore, he suggests, in line with Cohen's approach, that privacy is necessary for individual autonomy, which in turn is a prerequisite for individuals' ability to effectively participate in deliberative decision-making.[247]

This article takes Roberts' criticism a step further. Rather than

243. Andrew Roberts, *A Republican Account of the Value of Privacy*, 14 EUR. J. POL. THEORY 320, 336 (2015).

244. *Id.* at 335 ("While liberals are generally concerned about the effects that a loss of privacy will have on the autonomy of the subject, the focus of republican concern will be any unchecked inequality in power that is created by such a loss.").

245. *Id.* at 321.

246. *Id.* at 335.

247. *Id.* at 336–38.

framing the conversation around surveillance and privacy, we ought to frame it instead around domination and freedom. Much would be gained by reversing lenses. First, rather than looking at political freedom through the lens of privacy, privacy ought to be understood as one aspect in a broader discussion of freedom. Consequently, we ought to recognize that government technological control measures generate fundamental harm to human freedom, which encompasses a range of individual rights, including privacy and speech.[248] Second, rather than looking at government control through the lens of surveillance, we ought to discuss the much broader set of technological measures employed by governments to control their populations and curb opposition, among which surveillance is a key, but not a sole measure. The next two sections elaborate and defend this suggestion.

B. Reframing: Digital Domination and Human Freedom

Philip Pettit's republican theory offers an account that links freedom, domination, activism and the rule of law and is therefore helpful in drawing out the implications of governments' technological control measures. The central concept in Pettit's theory is human freedom, which he defines as non-domination. According to his conceptualization, individuals' freedom is impaired not necessarily when their liberty is interfered with, but when another has power over them which they cannot influence—a power to interfere at will.[249]

Pettit argues that a mixed constitution and a contestatory citizenry are necessary for securing freedom as non-domination. As he explains, the idea of a mixed constitution is to support the rule of law, or a constitutional order that would "deny control over the law to any one individual or body."[250] The contestatory citizenry is a civic complement to mixed constitution, aimed to check the various elements of government.[251] In other words, these are institutional and social mechanisms aimed to entrench and safeguard individual freedom understood as non-domination.[252] This article has insisted on the importance of recognizing the entire panoply of government control measures applied to activists and the fundamental harm to

248. *Cf.* PHILIP PETTIT, ON THE PEOPLE'S TERMS 8 (2012). Pettit links this thinking with Sen and Nussbaum's theory, saying that this sphere "may be identified, in contemporary terms, with the sphere of choice required for being able to function in the local society." (citation omitted).

249. *Id.* at 9.

250. *Id.* at 5.

251. *Id.*

252. *Id.* at 8.

freedom that is caused as a result. Pettit's triad of concepts helps demonstrate why this recognition is important. The reason is that activism (contestatory citizenry, to use Pettit's term) is a crucial oversight instrument meant to ensure the rule of law (a key goal of mixed constitution) and thereby to safeguard freedom (understood as non-domination).

The idea of a mixed constitution requires the division of the task of governance among different institutions, so that each works as a check on the others. It is meant to guarantee "a separation of powers, a sharing of powers and a balancing of powers,"[253] and to support the rule of law.[254] A mixed constitution is presumed to give voice to the people,[255] and would dispose the government to avoid triggering popular resistance.[256] Pettit refers in this discussion to Lon Fuller's book *The Morality of Law*, presumably alluding to a link which Fuller identifies between the criteria for law-making, on the one hand, and the law-maker's standing to expect the subject's cooperation, on the other hand.[257] As Fuller explains, without rule of law, a legal system has no standing to expect cooperation.[258] This non-cooperation may evolve into the popular resistance Pettit has in mind.

This section builds on Pettit's work to conceptualize government digital control measures as a form of arbitrary and uncontrolled domination, threatening not only the freedom of activists to whom the measures are applied, but also, consequently, the capability to engage in contestatory citizenry. The incapability further threatens the freedom of all citizens. In the next section, I return to Fuller and argue that governments' digital domination further jeopardizes the rule of law.

253. *Id.* at 221.

254. Understood as governance "in accordance with due process, not ruling by ad hoc decree but via public, general and prospective regulations." *Id.* at 221.

255. However, Pettit explains that "it would not be the voice of a single body, authorized to act as a spokesperson for the whole." *Id.* at 224. Rather, the people's voice, itself a multifaceted compound, would be delivered in the interaction between the different bodies participating in government. *Id.* at 220–25.

256. *Id.* at 219.

257. LON L. FULLER, THE MORALITY OF LAW 39–40 (rev. ed. 1969) ("As the sociologist Simmel has observed, there is a kind of reciprocity between government and the citizen with respect to the observance of rules. Government says to the citizen in effect, 'These are the rules we expect you to follow. If you follow them, you have our assurance that they are the rules that will be applied to your conduct.' When this bond of reciprocity is finally and completely ruptured by government, nothing is left on which to ground the citizen's duty to observe the rules.").

258. *Id.* at 39–40.

The idea of balancing power, one of the aims of a mixed constitution, comports well with Pettit's idea of a contestatory citizenry, which in turn has a special role in upholding the regime.[259] Pettit explains the importance of a "contestatory culture" among citizens, in which the people are disposed to resist government abuse.[260] One justification for the need for a contestatory citizenry is "the need to ensure that popular influence on government is not conditioned on the goodwill of government, or that of any third party."[261] This ideal does not have to be executed by every citizen; it is exemplified in the work of activists who operate as watchdogs over governments, and in their occasional recruitment of citizens on the basis of their particular concerns and passions.[262] Pettit views this contestatory spirit as a form of "civic virtue."[263]

Pettit differentiates the republican conception of freedom as non-domination from two competing conceptions: freedom as non-interference (which he identifies as the liberal conception of freedom) and freedom as non-frustration. The former characterizes a breach of freedom as an interference with one's preferred choice. The latter requires the "absence of invasive obstructions to any choice, preferred or unpreferred."[264] Domination, in contrast, is avoided where the person has control over the conditions under which an invasion of her choice is exercised.[265] For instance, the government's power to invade one's choices is not domination as long as mechanisms exist to ensure the person's ability to participate in checking that power.

This discussion underscores activism's role as an instrument of citizens' control over government power. Activism is intimately connected with the maintenance of the rule of law and, consequently, with securing human freedom. Legitimate government powers are premised on there being mechanisms for the public to control how this

259. PETTIT, *supra* note 248, at 222.

260. *Id.* at 225. He says further that such disposition must not only be present, but must also be "a matter of common awareness." He adds: "But this extra condition is likely to get fulfilled as a matter of course. It is hard to see how a mixed constitution and a contestatory citizenry could be present without its being manifest that they are present." However, as the discussion of government disruption and flooding indicates, it is no longer so clear that resistance would become a matter of common awareness.

261. *Id.* at 226.

262. *Id.* at 226–27.

263. *Id.* at 228. Although, to justify this characterization as virtue, Pettit says it must necessarily express a "commitment to living under an arrangement where all members of the community can share in a system of equal popular influence."

264. *Id.* at 64.

265. *Id.* at 59.

power is exercised, and activism is one of these mechanisms. Government power exercised without such control is a threat to human freedom. Therefore, undermining the conditions necessary to engage in activism that is critical of the government undermines a key safeguard of human freedom.[266] Moreover, systematic, widespread government interference with the freedom of activists has ramifications for the citizenry as a whole, because it threatens not only the freedom of the particular activist, but also the conditions for engaging in activism, which must be available to all citizens if they are to be free.[267]

Mapping this theory onto the practices discussed in Part I, the argument is that, seen in aggregate, the host of government technological control measures surveyed do not merely interfere with any particular activist's freedom, but also actively undermine the cyber infrastructure that enables modern activism. As already noted, the internet and social media have become a crucial and necessary work tool for twenty-first century activism. Activists use the internet and social media in order to produce and disseminate information and ideas,[268] generate public awareness, coordinate and mobilize public action by diverse actors,[269] and more. This situation is not one which could be rewound to pre-internet days. When governments weaponize the internet and social media against activists, deny their ability to organize and disseminate information online, and turn technology into a tool of surveillance, disruption and violence, they undo the conditions necessary to maintain an important check on government power. These measures therefore constitute the exercise of an uncontrolled power over human freedom. In other words, they constitute digital domination.

B.C. Newell makes a first attempt at bringing republican theory into these realms. He offers an argument about governments' use of surveillance technologies in policing and national security contexts, discussed through the concept of republican freedom.[270] Newell

266. *See also* Rahman, *supra* note 38, at 51–52 (synthesizing Pettit's republican theory with Progressive Era thinkers such as Dewey, and stressing the key importance of there being public institutions that make possible the organizing of collective action against concentrated power, focusing specifically, on private power).

267. John M. Alexander, *Ending the Liberal Hegemony: Republican Freedom and Amartya Sen's Theory of Capabilities*, 9 CONTEMP. POL. THEORY 5, 21 (2010); Rahman, *supra* note 38, at 57–59.

268. Cammaerts, *supra* note 8, at 7 (discussing the spread of the Arab Spring).

269. Segerberg & Bennett, *supra* note 9, at 200 (discussing the use of Twitter as both a networking agent in a transnational protest space and a window into it).

270. Newell, *supra* note 195.

reviews and underscores the importance of citizens' counter-surveillance of the state, through demands of transparency, freedom of information requests, requiring police officers to wear body cameras, and pursuing additional measures subjecting governments to the scrutiny of citizens. Such practices, he says, rebalance the power gap constituted by one party's observation of the other.[271] However, as the survey in Part I indicates, governments' use of technological tools has extended beyond these (at least theoretically) more innocuous contexts. Nevertheless, in line with Newell's approach, this article seeks to continue developing this conversation and use it to reveal the grave breaches of freedom that follow from government digital domination.

Pettit has been criticized for his characterization of liberalism.[272] Without necessarily buying into it, it is possible to read his conceptualization of freedom as compatible with a version of updated liberalism such as Sen and Nussbaum's. They have underscored the importance of one's autonomy to formulate and pursue her own life plan, and the necessity that she has the appropriate capabilities to do so if she is to be free.[273] Moreover, they identify providing all individuals with at least a basic level of these capabilities as a central goal of politics.[274] Nussbaum and Sen characterize their approach as a "friendly amendment to liberalism, rather than a wholesale replacement."[275] Pettit makes a similar claim, emphasizing that the main elements of republicanism, mixed constitution and contestatory citizenry, are echoed in liberalism's common endorsement of ideals like the rule of law, separation of powers and liberties of speech and expression.[276] He therefore suggests that the approach he defends may be characterized as republican liberalism or

271. *Id.* at 421–22. Such balancing can happen by activists' reciprocating additional measures of control, such as social media manipulation through hashtag hijacking, or disruption through DDoS attacks. For a study of technological resistance techniques, see Zar, *supra* note 34.

272. Pettit has been criticized for his account of liberalism and his underplaying of Rawls' political liberalism. *See, e.g.*, Paul Patton, *Political Legitimacy*, 18 CRIT. REV. INT'L SOC. & POL. PHIL. 661 (2015).

273. Their capabilities approach "looks not at actual functioning . . . but at the opportunities or 'capabilities' [people] have." Nussbaum, *supra* note 228, at 769 (stressing also a substantive, rather than formal, commitment to ensuring all individuals have such capabilities).

274. *Id.* at 769–70.

275. *Id.* at 772.

276. PETTIT, *supra* note 248, at 11. Alexander concurs. Alexander, *supra* note 267, at 6.

liberal republicanism.[277] John Alexander has argued that these two theories are in fact 'cousins': "[f]reedom, according to Pettit and Sen, is not merely the absence of interference from the state or fellow citizens but the presence of suitable conditions for the realization of citizens' capabilities."[278] I endorse this view, and it is against this background that this article underscores the usefulness of republican theory to the issues at hand.

C. The Rule of Trolls

As the survey in Part I demonstrates, governments have relied on citizens for tasks ranging from gathering information on fellow citizens to online bullying. Relying on volunteers, organized networks or cyberespionage firms, governments have often used these private actors in order to circumvent either the boundaries of their legitimate authority or the scrutiny of their citizens, or both.

Activists, journalists and academics have referred to such private, government-sponsored actors as trolls. However, this term has been used to capture a vast array of actions, mostly by private actors with widely differing degrees of relation to governments.[279] It has been used to encompass everything from entrepreneurial individuals reverberating on a large scale an otherwise legitimate government message, through government-organized groups making death and rape threats and hate speech against activists. Some have even included under trolling the arrest and prosecution of activists by the authorities.[280] We would do better to disassemble these various components. In the context of the present article, the purpose is to highlight instances where government mobilization of private actors poses a threat to the rule of law.

By recruiting private mercenaries in the form of cyberespionage firms and private cyber militias, governments have operated to shut down civil society critics and political opposition. The government, powerful as it is, cannot be everywhere. This fact is key in the idea of the panopticon, which is meant to compensate for the observers' inability to physically coerce each subject and therefore aims instead to nudge them into self-discipline via surveillance. But

277. PETTIT, *supra* note 248, at 11.

278. Alexander, *supra* note 267, at 5.

279. *See, e.g.*, NYST & MONACO, *supra* note 85; ONG & CABAÑAS, *supra* note 132; N. Bulut & Erdem Yörük, *Digital Populism: Trolls and Political Polarization of Twitter in Turkey*, 11 INT'L J. COMM. 25 (2017); Morla, *supra* note 176.

280. NYST & MONACO, *supra* note 85.

when political activity relocates to cyberspace to such a degree as it does today, it becomes possible to be almost everywhere. By combining the forces of government institutional power and technological sophistication together with rogue technological firms, unofficial informants and bullies, governments are able to bypass both the technical and the legal limits of their authority.

In this way, governments' reliance on private actors threatens not just targeted activists, but also the rule of law. In his famous battle with H.L.A. Hart, Lon Fuller defended the position, voiced by Gustav Radbruch, according to which the Nazi system was not, properly so called, a legal system.[281] One of Fuller's more compelling points in this debate was stressing that the most important affronts to the rule of law by Hitler's government were reflected in the fact that "when legal forms became inconvenient, it was always possible for the Nazis to bypass them entirely and 'to act through the party in the streets.'"[282] Here, government reliance on private mercenaries and private militias to monitor and curb political opposition is the cyber equivalent of acting "through the party in the street," albeit virtual rather than physical ones. In a modern, networked world, it is similarly a grave threat to the rule of law.

CONCLUSION

Many of the government practices surveyed in this article may not seem new to the reader. In addition to the many stories covered daily by the press, the likes of China's Social Credit System has recently received popular representation in a *Black Mirror* episode, and George Orwell's *1984* has made a comeback to the 'Best Seller' lists.[283] Nevertheless, there is an alarming impact to considering in aggregate not only the massive surveillant assemblage to which we are all subject, but also the digitally-induced authoritarian practices that are increasingly its companions. Governments are not only watching, but are also actively silencing, drowning out, exercising their sovereign coercive powers over, and bullying opposition actors. In an era of democratic backsliding, the technological empowerment of

281. Gustav Radbruch, *Statutory Lawlessness and Supra-Statutory Law (1946)*, 26 OXFORD J. LEGAL STUD. 1, 7 (2006).

282. Lon L. Fuller, *Positivism and Fidelity to Law: A Reply to Professor Hart*, 71 HARV. L. REV. 630, 652 (1958).

283. Kimiko de Freytas-Tamura, *George Orwell's '1984' Is Suddenly a Best-Seller*, N.Y. TIMES (Jan. 25, 2017), https://www.nytimes.com/2017/01/25/books/1984-george-orwell-donald-trump.html [https://perma.cc/LVC8-JUNA].

states has become a key threat to constitutional arrangements that are meant to guarantee against authoritarianism.

This article should be read as a call for engagement. It aims to expose the grave effects of digital domination, particularly when applied to civil society and political opposition activists, but also, consequently, for all of us. The quantitative transformation of government capabilities induced by technology is significant enough to constitute a qualitative leap, as well.

Recognizing this threat does not necessarily lead, in my view, to a conclusion that governments ought never to engage in monitoring of online activity or act on the resultant information. Clearly, governments do and should continue to do so on a range of issues from cyberbullying to violent crime and national security. Nevertheless, recognizing the threat of digital domination to freedom, engaged citizenry and the rule of law require starting a conversation about how to resist such domination and how to minimize its threat. This article strives to take a first step in outlining the toolkit used by governments. The appropriate response may differ between each of these categories. What could be done to offset this threat? A comprehensive review of this question is beyond the scope of this article. However, several tentative directions may be suggested.

First, the persistent optimism, resilience and courage that are displayed by activists in the face of government control measures should inspire our thinking going forward. Digitally informed resistance, the likes of which Hong Kongers have recently showcased, is one tactical response.[284]

Second, stricter public oversight of governments' adoption and deployment of sensitive technologies is required. This is the takeaway from Newell's proposition to increase demands of transparency from the government and to seek to uncover information on authorities in order to rebalance the power gap engendered by government surveillance.[285]

Third, regulation must be put in place to guide and limit decisions on adoption and use of sensitive technologies, and their proliferation across government departments. San Francisco and other U.S. cities have recently elected to ban the use of facial recognition software due to its grave implications.

Fourth, constitutional law offers some tools to apply to prevent governments' use of pilot programs to introduce technologies of control through experimental application to marginal communities or

284. For more on technological resistance, see Zar, *supra* note 34.

285. Newell, *supra* note 195.

under the guise of national security.

Fifth, international action is called for. The proliferation of oppressive technologies across borders should be monitored, disclosed and justified domestically and internationally. As suggested by UN Rapporteur David Kaye, the sale of cyberespionage software should be subjected to close scrutiny and to an immediate moratorium.

Finally, the scholarly discussion of these issues should seek to draw in additional perspectives. Specifically, more constitutional scholars and international lawyers, as well as legal and political philosophers, should make it a priority to become technologically proficient and join the conversation in order to address the threat that technology—combined with a receding respect for democracy—carries for human freedom, democratic institutions and the rule of law, as well as the appropriate responses. International law as well as constitutional law should become engaged with monitoring and curbing abuses.

How is human freedom impacted by the rise of the technologically-fortified state? Does governments' technological empowerment contribute to the global trend of democratic backsliding, and if so, in what ways? Relatedly, how does technology impact individuals' ability to utilize law in order to pursue their own goals and shape their lives? How does it affect their ability to exercise their human rights? And what are the implications of technologically-induced public-private collaborations for the rule of law? These are questions that this article only begins to probe. Hopefully, it will encourage others to join the conversation.