Democracy on the Margins of the Market: A Critical Look Into the Privatisation of Cyber Norm Formation

DRAFT VERSION V0.1

Emma Ahmed-Rengers
University of Birmingham
emr985 AT student.bham.ac.uk

Mansoor Ahmed-Rengers
University of Cambridge
mansoor.ahmed AT cl.cam.ac.uk

1 Introduction

When it comes to responsible behaviour in cyberspace, there are two questions we ought to ask ourselves: Who are the actors who behave in cyberspace? And who can legitimately set standards for "responsible behaviour" of those actors?

In the existing literature on cyber policy, these questions have typically been approached from two angles. The first angle is grounded in international law. This strand of literature looks into the applicability of international legal doctrines in cyberspace; the formation of customary law; and analogies between cyberspace and more traditional international legal concepts like the high seas and outer space. International law is undoubtedly a large component of the cyber norms landscape. Yet focussing on narrow legal debates on the applicability of treaties, the formation of custom, and the legal standing of actors implies a taken-for-granted existing legal structure and its inherent statist bias, which may fail to recognise broader social, technological, and economic trends.

The second angle is a descriptive, realist inquiry into who has power in cyberspace. This type of research looks into the strategies that different actors use to secure their seat at the negotiating table, and the arguments they use to legitimise their authority. The advantage of this research is that it transcends narrow legal debates, and is therefore able to reckon with broader societal developments, such as the rise of private actors in cyber norms formation. However, while the legal approach evaluates certain behaviour from the point of view of legal normativity, this second strand of research often fails to comment on normative, political legitimacy of actors.

This paper aims to build and critically reflect on both of these strands of

literature. We criticize the international legal focus on states as the main actors in cyberspace. Moreover, we express scepticism about the appropriateness of international legal doctrines like the use of force and international humanitarian law (IHL) in the context of cyber norms formation. We argue that these doctrines fail to reckon with the immense influence of private actors; most notably corporations. We then critically reflect on the existing scholarship on private actors in cyber norms formation. We argue that the involvement of private actors in cyber norms formation must be seen and evaluated in the context of neoliberalism, corporate social responsibility, and surveillance capitalism. As such, the involvement of private actors in the cyber norms landscape is part of a larger trend towards the hollowing out of the state, a move away from law and accountability mechanisms, and the erosion of democratic rights.

We specifically argue that the neoliberal turn in the cyber norms debate is harmful in the context of large corporations in cyberspace, as the pervasive logic of surveillance capitalism threatens our democracies. Large tech corporations cannot be said to be working for the common good, and their normative influence can therefore not be assumed to be benevolent or legitimate.

2 Cyber Norms and International Law

As cyberspace crosses international borders, and does not fall within the sole jurisdiction of one nation state, international law applies (Boeke and Broeders 2018, 73; Koh 2012, 3; Schmitt 2012, 16). More specifically, as cyber capabilities are perceived as a national security asset, cyberspace is often associated with the "legal frameworks regulating military conduct during war and peace." (Boeke and Broeders 2018, 73) In his seminal speech, US State Department Legal Adviser Harold Koh argued that cyberspace is regulated by IHL. Although Koh did mention that the law of armed conflict is not the only body of international law that applies to cyberspace, and that human rights should also be considered (Koh 2012), statements like the following illustrate his militaristic focus:

> "[I]f the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force." (Koh 2012, 4)

> "A state's national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof." (Koh 2012, 4)

This same militaristic focus is echoed in the Tallinn Manual on the International Law Applicable to Cyber Warfare (Schmitt 2013), which also prioritises the applicability of jus ad bellum and IHL in cyberspace. Michael Schmitt, Director of the Tallinn Manual Project, emphasised that the "congruency between the U.S. Government's views, as reflected in the Koh Speech, and those of the International Group of Experts is striking" and "significantly enhances

the persuasiveness of common conclusions." (Schmitt 2012, 15)

This seemingly overwhelming consensus on the relevance of IHL for cyberspace is somewhat bewildering, considering that IHL has no actual bearing on the majority of activity in cyberspace. Strictly speaking, IHL only becomes applicable in the context of armed attacks of state actors against other state actors[1]. This has two components: 1) a threshold of violence ("armed attack") must be reached, 2) this violence must emanate from a state actor and must be inflicted on another state actor. The problem with trying to apply IHL in cyberspace is that typically neither of these conditions are met.

Firstly, states have never considered any cyber operation as reaching the threshold of violence that makes IHL relevant (Mačák 2017, 884-885[2]). Most cyber activity actually occurs "outside the parameters of international humanitarian law" (Boeke and Broeders 2018, 74). The focus on cyber operations which cause physical damage, injury, or death, distracts from the more subtle forms of control that cyber operations produce. Non-military, peacetime cyber operations can still have considerable negative impact on citizens' rights; most notably in the context of (algorithmic) surveillance and espionage.

Secondly, the fact that IHL regulates inter-state violence means that this whole body of law has little bearing on the activities of private actors, which are crucial actors in cyberspace. Private actors own a significant share of the tools, infrastructure, capital, and knowhow that make up cyberspace, and therefore exercise immense power. In addition to this physical and intellectual power, private actors also increasingly exercise normative power, as will be explained in the next section.

If IHL actually has little relevance to governing cyberspace, then why has it received so much attention? As a US government official, Koh's motivations for laying out this specific legal framework are clear and explicit:

> "[Compliance with international law] frees us and empowers us to do *things we could never do without law's legitimacy.* If we succeed in promoting a culture of compliance, we will reap the benefits. And if we earn a reputation for compliance, the actions we do take will earn *enhanced legitimacy worldwide* for their adherence to the rule of law" (Koh 2012, 11, emphasis ours); "in a way that more fully *promotes our U.S. national interests*" (Koh 2012, 12, emphasis ours).

Koh chose to emphasise international humanitarian law (which only applies in a very limited range of scenarios) over international human rights law (which applies to *all* state action). He then argued that compliance with this specific legal framework benefits US national interests, as it grants legitimacy to US

1. Common Article 2 of the Geneva Conventions states: "the present Convention shall apply to all cases of declared war or of any other *armed conflict* which may arise *between two or more of the High Contracting Parties*" (emphasis ours)

2. "Crucially, no cyber operation – including Stuxnet (...) – has ever been considered to amount to use of force by any state, whether by a victim or a bystander." Mačák does note, however, that all members of the international group of experts associated with the Tallinn Manual do consider Stuxnet as an instance of the use of force.

actions in cyberspace which "we could never do without law's legitimacy" (Koh 2012, 11). These words might not have aroused suspicion when they were spoken in 2012, but they acquired new significance in light of Edward Snowden's 2013 revelations of controversial US global surveillance programmes.

The US government is not the only actor in the cyber norms space who used the language of IHL to legitimise its own actions. Microsoft, in its attempts to influence cyber policy, fully embraced the militarised narrative of cyberspace by calling for a "Digital Geneva Convention," and conceptualising Microsoft's role as a "neutral Digital Switzerland" (Smith 2017). The association with peace, neutrality, and humanitarianism has "clear reputational benefits" (Gorwa and Peez 2020, 274) for Microsoft, without imposing any substantive legal obligations on the company or restricting its usual operations. In this manner, Microsoft can sell its so-called cyber defence products to all sides in this hypothetical cyberwar—as it has done and continues to do (US Department of Defense 2019; Targett 2020; Bodhani 2016; Novet 2020)—while still maintaining an air of benevolence. If we are to use militarised language, Microsoft ends up resembling not a neutral Switzerland here but rather an arms dealer.

To summarise, international humanitarian law has been emphasised as the relevant normative and legal framework that constrains cyber operations. IHL does not restrict peacetime operations and most operations of private actors, and therefore has had little impact on actual cybersecurity. Yet, talk of humanitarianism confers reputational benefits on the actors who espouse it. Both states and corporations can use the militaristic conception of cyberspace to legitimise their actions without reference to tricky concepts such as surveillance, privacy, and transparency.

Despite the lack of relevance of IHL, and the ensuing gap in legal protection in cyberspace, states have been reluctant to create additional international legal standards for cyberspace (Boeke and Broeders 2018, 75). Instead, they operate under the assumption that "whatever is not explicitly prohibited by international law is allowed" (Boeke and Broeders 2018, 77). This lack of legislative initiative and normative leadership from states has opened up space for non-state actors, most notably corporations, to formulate their own cyber policies and promote themselves on the global stage as legitimate norm-makers.

The following sections consider how this relative absence of the state and its legislative power in cyberspace, and the subsequent rise of private actors, have been described in cyber norms literature. Moreover, we aim to show that these descriptions are not ideologically neutral, but rather fit within a larger history of neoliberalism and global capitalism, which have found fertile soil in cyberspace. We then argue that a neoliberal approach to cyber norms is problematic in the context of surveillance capitalism, which seeks to extract economic value from our behaviour and undermines the foundations of our democracies.

3 The Retreat of the State and the Rise of Private Actors

Different authors attribute the relative absence of the state in the formation of cyber law to different causes. Kubo Mačák (2017) argued that states are intentionally refraining from legislating in the cyber domain, as they resist the drafting of treaties and avoid creating customary law by shrouding their cyber operations in secrecy. According to Mačák, this lack of legislation "has left a power vacuum, triggering a number of non-state initiatives seeking to fill it" (Mačák 2017, 881).

Other authors attribute the lack of legislation not to intentional state behaviour, but to deficiencies of state actors which make them unable to legislate effectively, such as their slow and bureaucratic nature (Hurel and Lobato 2018, 66[3]), the lack of consensus (Eggenschwiler and Kulesza 2020, 255[4]), and the lack of resources (Hurel and Lobato 2018, 66[5]).

This alleged absence or incompetence of the state has led various authors to conclude that there is "limited statehood" (Gorwa and Peez 2020, 270) in cyberspace, creating space or even necessity for corporate actors to contribute to the norm-making process. Authors speak of "a shift in global regulation from state-centric forms of steering toward new non-territorial, multi-actor modes of governance"(Eggenschwiler and Kulesza 2020, 252-253), "state-firm diplomacy"(Hurel and Lobato 2018, 69), "governance without government"(Hurel and Lobato 2020, 289), and "decentralized governance processes" (Hurel and Lobato 2020, 292) in which the involvement of corporate actors is seen as "simply essential" (Hurel and Lobato 2020, 294) and "an absolute necessity"(Fairbank 2019, 395).

To explain this governance trend, we need to address both the demand and the supply of private authority. The aforementioned explanations of the retreat of the state seem to account for the demand for private authority. The first explanation of state unwillingness portrays the state as a competent but absent actor, while the second sees the state as a present but incompetent actor. Although these explanations seem contradictory, the state that intentionally refrains from legislating and the state that is seen as too incompetent to legislate can both be viewed as adhering to the "rules and scripts of neoliberalism" (Shamir 2010, 545). The neoliberal conception of the minimal state dictates that states ought to interfere with private authority as little as possible, and that market solutions must be sought for social and political problems. Both the absent and the incompetent state fit within this neoliberal framework.

The current supply of private authority is mostly attributable to Microsoft. Its aforementioned "Digital Geneva Convention" is part of a larger, successful strategy to become a "quasi-diplomatic" (Hurel and Lobato 2018, 71) actor "at

3. "negotiating treaties can be a slow and cumbersome process, ill-suited to fast-changing issues like cybersecurity and Internet governance"

4. "progress-inhibiting contention at the intergovernmental level"

5. "Governments may not be the best or only actors to be making rules in this area since so much of the technology is in private hands"

the head of the table" (Gorwa and Peez 2020, 273) of cyber norm negotiations. As discussed before, this position gives Microsoft an opportunity to improve its reputation as a trustworthy actor. Moreover, it puts Microsoft in a position to effectively influence the norms guiding behaviour in cyberspace, and thereby to protect and promote its own products and services (Fairbank 2019). Microsoft's behaviour and its justifications seem to be in line with neoliberal ideology, as they link their strategies to general welfare, convincing citizens that their interests are aligned with those of tech corporations, and claiming that promoting commerce is "good for everyone" (Hurel and Lobato 2020, 296).

The shift to a governance model in which corporations play a central role in standard-setting is tightly linked to the concept of corporate social responsibility (CSR). CSR is a phenomenon whereby corporate actors go beyond their legal obligations and seemingly beyond their profit maximisation goals by creating their own social policies, typically "marked by the creation of multiple private and self-regulatory tools" (Shamir 2010, 532). Microsoft's behaviour falls squarely within this category. The "policy" documents it has produced set self-regulatory standards for the industry (Gorwa and Peez 2020).

On the face of it, CSR seems to be incompatible with capitalism, as it seems to diverge from the capitalist conception of the corporation as an entity that is driven by profit maximisation. However, Ronen Shamir convincingly argued that CSR and the "governance turn" (Shamir 2010, 533) are consequences of global capitalism's ability to transform not only "the means and relations of production, but also the means and relations of political authority" (Shamir 2010, 546). He showed that the governance turn transforms the political authority and legitimacy in favour of corporate power, and to the detriment of state power, thereby perpetuating neoliberal ideology. According to Shamir, it does so through the economisation of authority and the concept of the moral corporation. In the following sections, we use these concepts to explain and critique the retreat of the state and the rise of private actors in the cyber norm landscape.

3.1 The Economisation of Authority

The "economisation of authority" refers to a way of thinking about authority that is marketised. Traditional government is seen as a centralised, hierarchical, rule-based structure of authority (Shamir 2010, 534), which exists outside the realm of market forces. As traditional state authority is not derived from market value, states can act in ways that are nonsensical from a market perspective, such as providing free education or healthcare for all citizens. If public action is not dictated by market logic, this allows state authorities to act for non-economic reasons. This view of state authority therefore recognises that not all domains of human action have to be organised according to market logic. In this view, public authority is legitimised through political process and political normativity, while private authority is derived from the separate domain of economic market value.

Governance models of authority claim to transcend the distinction between public and private, and introduce "multistakeholder task-sharing policy initia-

tives" (Shamir 2010, 534) which invite both public and private authorities to the same negotiating table[6]. Authority is no longer centralised, but fragmented, and different actors from different domains compete for legitimacy and influence. This not only means that the policy-making process includes voices which represent corporations operating according to market logic (centralised models of democratic state authority also incorporate these voices through the democratic process), it also means that "the very notion of authority" (Shamir 2010, 536) is subjected to market logic. Actors from the public and the private domain compete for authority in a market-like fashion, arguing that they are more competent, more efficient, faster, or more equipped than other actors, thereby side-lining the question of who is more legitimate from a normative point of view.

We can recognise this exact phenomenon in the case of Microsoft's involvement in cyber norms and how Microsoft's involvement in the norm-making process has been legitimised through the literature describing it. The term "cyber norms" implies a normative, political aspect. Deciding who gets to have a say in the definition of norms is a political, ideological task. Granting equal legitimacy to public and private actors in this norm-making process is therefore an ideological move, which lets public and private authority compete on the terms of private authority. Equating public and private authority and pitching them against each other in an imagined level playing field of authority portrays the political realm as subsumed under the realm of market forces. This is therefore an ideological move grounded in neoliberalism.

This move from centralised government models to fragmented governance models comes with a move away from the traditional tools of government; most notably law (Shamir 2010). Law is seen as a tool that is too slow, too inefficient, too contentious, or too hierarchical to adequately deal with the formation, application, and enforcement of norms. Governance instead opts for "quasi-legal arrangements" (Shamir 2010, 534), which use the style and language of law, but do not include the characteristics that make law law, such as enforceable sanctions, authoritative processes for interpretation, requirements of transparency and the giving of reasons, and other traditional accountability mechanisms. Even framing the debate in terms of cyber norms, rather than cyber law, is another strategy for promoting the rise of private actors (who do not have law-making authority) in the debate and contributing to the demise of the state and its tools of governing.

The economisation of authority and the retreat of law are reflected in discussions on Microsoft's involvement in the cyber norms debate. Microsoft is often described as an actor which has equal standing to states. A blogpost from the UNHCR Innovation Service states that:

> "[T]echnology companies would be required to take on a *stronger role in the existing international state system and its global institutions*, like the United Nations, in helping to *define matters of human rights and humanitarian protection* in the digital age. (...) *Tech compa-*

6. "governments are reconfigured as one source of authority among many, operating in a vast and diversified competitive market of authorities that legitimately includes as equal participants authorities such as corporations" (Shamir 2010, 535)

> *nies – alongside states*, humanitarian actors and civil society – will need to help *define* what actions constitute cyber threats or attacks, and therefore *who should be afforded rights and protection under international law.* (...) The Digital Geneva Convention initiative is an exciting call to action for defining new rights and responsibilities and re-tooling the existing system to cope with the realities of the 21st Century." (Guay and Rudnick 2017, emphasis ours)

The claim that tech companies should be able to define rights under international law alongside states suggests that corporations and states are both legitimate actors operating in the same domain. Robert Gorwa and Anton Peez described Microsoft President Brad Smith as a "global cybersecurity statesman" (Gorwa and Peez 2020, 264). Luise Marie Hurel and Luisa Cruz Lobato described Microsoft as trying to advocate for sharing responsibilities between themselves and states, in a process of "state-firm diplomacy" (Hurel and Lobato 2018, 69). Jacqueline Eggenschwiler and Joanna Kulesza advocated for "joint steering efforts and share[d] responsibilities with sovereign authorities" (Eggenschwiler and Kulesza 2020, 256). Equating Microsoft to a diplomatic actor confers the legitimacy of statehood on them, without imposing any of the legal and moral obligations that come with actual statehood.

While Microsoft is described as an entity which can provide "high-level expertise" (Hurel and Lobato 2018, 69), "responsiveness to technological change" (ibid), and efficiently close the "global governance gap" (ibid), state regulation is described as "slow and cumbersome" (Hurel and Lobato 2018, 66), "ill-suited to fast-changing issues like cybersecurity" (ibid), and "progress-inhibiting"[7] (Eggenschwiler and Kulesza 2020, 255). These criteria for who is a legitimate norm-maker only make sense in an economised approach to authority. If we ask ourselves who is quick, efficient, has the resources, and promotes in progress economic terms, corporations seem to be better suited for the task. From the point of view of the market, being slow and bureaucratic is detrimental to success.

However, if we approach authority in norm-making from a non-market, political perspective, we would emphasise entirely different virtues. State action may be slow and bureaucratic because it is formed through a democratic process which involves many constitutional safeguards to protect the rule of law and civil rights, and requires the state to carefully balance the many interests of its pluralist population. When it comes to norm formation in democratic states, speed and efficiency are not the main virtues. Democratic compromise, human rights, and the rule of law are. Corporations do not have any procedural or substantive safeguards in place to ensure that they pursue the common good. The assumption that qualities which are valued in markets, like speed, efficiency, and resources are equated with the common good and "state-like" legitimacy, is a neoliberal move which side-lines democracy, human rights, and the rule of law. It is therefore a clear manifestation of the economisation of authority.

The hollowing out of the traditional tools of government becomes clear from

7. These perceptions reflect what Shamir calls the "dogma of state failure" (Shamir 2010, 535)

discussions about the quasi-legal nature of Microsoft's actions. Eggenschwiler and Kulesza described Microsoft's self-regulatory practices as "lawlike." (Eggenschwiler and Kulesza 2020, 256) Similarly, Mačák described the practices as a "more multi-lateral and inclusive" "law-making process" (Mačák 2017, 892). If one chooses to emphasise how much Microsoft's efforts resemble law, one must also highlight in which important ways the efforts differ from law. The aforementioned descriptions fail to acknowledge that Microsoft's self-regulatory initiatives lack the procedural legitimacy that democratically created law possesses, and the substantive legitimacy that comes with actual rule of law safeguards. The economisation of authority in the realm of cyberspace is not a recent phenomenon attributable solely to Microsoft, nor is it solely attributable to corporations in general. States themselves can be said to be complicit in this process. Stephen Gill argued that the intensification of rivalry between states on the increasingly globalised market, in combination with the economic slowdown which followed the 1973 oil crisis, created a "growing tendency toward the increasing use of surveillance capabilities by liberal democratic states to regulate the new market society and to exercise social control in a period of rapid social change" (Gill 1995, 13).

The economic slowdown in the 1970s was followed by the neoliberal Reagan and Thatcher era in the 1980s, which was characterised by marketisation and privatisation (Gill 1995). While the state delegated authority to private actors, it also invested heavily in surveillance technology in order to build and exploit databases to exercise a new form of social control. As neoliberal state actors were not reluctant to work alongside corporate actors, and private enterprises were seeking to capitalise on new surveillance technologies, public and private data collection and analysis became difficult to separate from each other. Public and private actors shared an interest in acquiring detailed information on economic and social behaviour of their own and foreign citizens, in order to manage risks created by increased reliance on international markets and the "heightened competitiveness of the global political economy" (Gill 1995, 20-22).

Gill highlighted how the Clinton administration actively sought to foster a connection between government intelligence and business, by arguing that:

> "The preeminent threat to US national security now lies in the economic sphere. (...) This means we need better economic intelligence. The United States does not want to be surprised by such worldwide developments, new mercantilist strategies, sudden shortages of raw materials or unfair and illegal economic practices that disadvantage the country. [There needs to be] a more symbiotic relationship between the worlds of intelligence and business." (Gill 1995, 34)

Shoshana Zuboff (2018) described how the "elaboration and implementation of the neoliberal economic paradigm" (Zuboff 2018, 31) in the US fostered contempt for regulation. Moreover, even though there were some efforts to regulate the activities of Google in 2000, these were dropped after the 9/11 attacks in 2001 (Zuboff 2018, 113). The 9/11 attacks created a "new interdependence between public and private agents of information dominance" (Zuboff 2018, 115),

and resulted in a deliberate blurring of the boundaries between public and private in order to promote national security. It is also worth noting that Google and the intelligence community share a history of close cooperation; early research into Google's web crawling technology was funded by grants from the CIA and the NSA (Nesbit 2017). While the state was seeking solutions to the threat of terrorism, tech corporations sought new ways to exploit data for commercial gain. Both shared a commitment to datafication, digitalisation, and automation in an effort to increase certainty and to pursue the promise of guaranteed outcomes, whether they were public or private. Zuboff argued that it is specifically Western democratic states that move with and through corporations to build a surveillance apparatus that benefits both the state and the corporations (Zuboff 2018, 394).

These historical developments (amongst others) created an environment where states fear being outcompeted by other states on both the economic and the security front, and where the lines between those two fronts are blurred.

This is most clearly visible in the "arms race" (Yeung and Lodge 2019, 28) that is associated with artificial intelligence (AI). The winner of the imagined arms race is promised substantial "political, military, and economic power" (ibid). States embrace AI-powered tools in an increasing number of domains, thereby "increase[ing] the size of cyberspace" (Cavelty and Wenger 2020, 23) and "link[ing] cyberspace to more policy domains" (ibid). The more activities are dragged into the cyber domain, the more data is collected about the economy, the military, the administration, and "society overall" (Cavelty and Wenger 2020, 15), creating new opportunities for cyberattacks compromising new computer systems and new data. Widespread adoption of AI creates new vulnerabilities and therefore more demand for cybersecurity. As both AI and cybersecurity tools are commonly developed in the private sector, states will become even more dependent on tech corporations (Cavelty and Wenger 2020, 23).

This competitive arms race that creates even tighter relationships between states and tech firms can be linked to the economisation of authority. According to Shamir, global capitalism creates states which themselves come to act as corporations engaged in market competition with others, and which "put their legal and administrative capacities at the service of transnational markets" (Shamir 2010, 535) – in this case, the transnational market for data and intelligent software.

3.2 The Construction of the Moral Corporation

In the previous section, we saw the dynamic by which authority can be economised in discussions about cyber norms. According to Shamir (2010), economisation of authority is often a response to a crisis of legitimacy of capitalism. In response to a perceived legitimacy crisis, corporate actors create a market for authority, through the economisation of authority as previously described. They then create demand for themselves on that market of authority by constructing an image of the "moral corporation." In Shamir's words:

> "[C]apitalism relies on critiques in order to alert it to threats, to neu-

> tralize opposition, and, moreover, to develop new moral justifications for the increase of profitability. (. . .) [Capitalism must demonstrate] a positive improvement in terms of justice (. . .) [and] incorporate some of the values in whose name it was criticized." (Shamir 2010, 537)

The notion that corporations seek to transform the very notion of political authority to their own advantage is echoed by Hurel and Lobato, who argued that corporations seek to "stretch the boundaries of [their] legitimacy" (Hurel and Lobato 2020, 304) through engagement with cyber norms, and may "work as meaning managers" (Hurel and Lobato 2018, 67).

Gorwa and Peez (2020) argued that the legitimacy crisis which sparked Microsoft's campaigns for cyber norms was caused by the Snowden revelations in 2013. Snowden's information revealed an "unusually close cooperation between the NSA and Microsoft" (Gorwa and Peez 2020, 271), which left Microsoft with "little choice but to go on the offensive and enter the fray as a norm entrepreneur" when it faced heightened scrutiny for having been involved in controversial and illegal (*United States of America v. Moalin* 2020) global surveillance (Gorwa and Peez 2020, 273).

In order to deflect criticism connected to their involvement in the surveillance activities revealed by Snowden, Microsoft published statements promoting the values in whose name it was criticised: "confidence in the security and privacy of online communications" (Smith 2013a) and "the personal freedoms of people"(Smith 2013b).[8]

Microsoft is still a widely trusted corporation, and some of the cyber policy literature on Microsoft's operations expresses sympathy for its "moral" behaviour. Nancy Fairbank, for example, stated: "It is very difficult to explain the motivations of norm entrepreneurs without reference to empathy, altruism and ideational commitment" (Fairbank 2019, 383). Eggenschwiler and Kulesza expressed even stronger support for Microsoft, describing it as one of the "benevolent non-state actors (. . .) that actively seek to promote appropriate conduct in cyberspace" (Eggenschwiler and Kulesza 2020, 246), and "deserve particular analytical attention in terms of fostering international peace, security, and stability" (Eggenschwiler and Kulesza 2020, 248). They also claim that Microsoft's behaviour is "grounded in the belief that deep-rooted collaboration among states, and between states, the private sector and civil society is needed to curb nefarious doings in the digital realm" (Eggenschwiler and Kulesza 2020, 250). Similarly, the UNHCR Innovation Service blog speaks of "Smith's bold vision (. . .) – a commitment to non-proliferation of cyber weapons, and international processes for dealing with cyber-attacks aimed at civilian populations"(Guay and Rudnick 2017).

8. At about the same time as Microsoft was making these statements, they pushed updates to the Windows operating system that introduced many forms of data collection and telemetry, and in most cases, made them mandatory. This move was widely criticised by the computer security community as eroding both the privacy and digital freedoms of computer users; the amount of telemetry and data collection in Windows has only gone up since (Kalia 2016).

By presenting itself as a moral actor with moral goals, Microsoft successfully deflected a threat to its profits and simultaneously established itself as a legitimate actor on the market of authority. In doing so, it even attempted to legitimise itself at the expense of the state they had cooperated with, by claiming that "[g]overnments have put this trust [in technology] at risk" (Smith 2013a) and "government snooping potentially now constitutes an 'advanced persistent threat"' (Smith 2013b). At least some of the scholarship describing Microsoft's norm advocacy reinforces the image of Microsoft as a moral corporation, and thereby—perhaps inadvertently—echoes a corporate PR campaign which was meant to save a corporation from the consequences of its immoral behaviour.

4 Surveillance Capitalism and the Dispossession of Rights

The previous sections showed that the domain of cyber policy is at risk of being captured by neoliberalism, the hollowing out of law, and the bypassing of democracy. This can be seen in the narrative of the demise of the state and the rise of private actors, which follows the script of the economisation of authority, presenting private authority as equivalent or superior to public authority in cyberspace. We also see it in the move away from law and its associated accountability mechanisms in favour of non-binding norms and self-regulation, reflected in the term "cyber norms" itself. Some of the scholarship on Microsoft as a norm entrepreneur reinforces this neoliberal narrative by presenting Microsoft as a moral corporation.

The neoliberal move in normative thinking about cyberspace is problematic in the economic dynamics seen in the context of cyberspace. Neoliberalism typically links market forces to the common good. However, Zuboff (2018) has convincingly argued that market forces within cyberspace are not geared towards the common good. To the contrary, she described the phenomenon of "surveillance capitalism" as a dominant economic logic that operates in cyberspace, which "unilaterally claims human experience as free raw material for translation into behavioural data" (Zuboff 2018, 8). This behavioural data is then used to predict and shape our future behaviour to the benefit of corporations. Surveillance capitalism is grounded in "instrumentarian" power, which is geared towards "shap[ing] human behavior towards others' ends" (ibid). According to Zuboff, the violation of civil and political rights, most notably the right to privacy, is a "feature not a bug" (Zuboff 2018, 50) of "most internet-based business" (Zuboff 2018, 10). Surveillance capitalists have constructed a "pervasive global architecture of ubiquitous computing" (Zuboff 2018, 309) which combines neoliberalism with "radical behavioralism" (Zuboff 2018, 362); a theory that reduces individuals to their observable behaviour and prescribes methods to modify that behaviour.

Zuboff argued that the control that corporations seek to exert over our behaviour through our data, and the subsequent loss of privacy and individual autonomy leads to a loss of individuality. A sense of individuality and control over our own behaviour is crucial for us to act as moral agents, which is cru-

cial for us to fulfil our role as citizens in healthy democracies (Zuboff 2018, 470).

By converting the experiences and behaviour of individuals into raw data for statistical analysis meant to maximise corporate profits, surveillance capitalism prefers "populations" (in the clean, statistical sense) over "societies" (in the messy, political sense) (Zuboff 2018, 428). Zuboff sees this "obliteration of politics" as the definition of "tyranny" (ibid). Karen Yeung and Martin Lodge share this concern "about the ways in which corporate and state power may intervene with constitutional rights in ways that potentially threaten the very socio-technical foundations upon which individual freedom and human rights are anchored" (Yeung and Lodge 2019, 13).

In light of these warnings, it might be sensible to carefully and critically consider the role that we, as a society, bestow on corporations in the process that is meant to produce normative standards for cyberspace. States ought to reclaim their legitimate space in the cyber norms debate, and defend the common good over private interests. Corporations are indeed an integral part of society, and ought to be heard in the process of standard-setting; just like any other interest group in society. However, as large tech corporations only represent a narrow set of interests (those of surveillance capitalists), they cannot legitimately negotiate with representative governments as equals, and their actions should be subjected to binding, democratic law which holds them accountable to the public.

5 Conclusion

Now let us return to the two questions asked at the beginning of this paper: Who are the actors who behave in cyberspace? And who can legitimately set standards for "responsible behaviour" of those actors?

Regarding the first question, it has become clear that the traditional focus on state behaviour in international law and international relations does not sufficiently capture the complexities around authority and legitimacy in the cyber norm-making process. As private actors exercise immense power in cyberspace and in cyber norm formation, we must consider the activities of corporations. The international legal framework which emphasises military use of cyberspace does not reckon with the usual operations of corporations and therefore create a gap in legal protection.

Regarding the second question, we have shown that the *political legitimacy* of corporations in the exercise of defining normative standards for cyberspace *cannot be assumed*. Wherever it is assumed, it is likely that this is done on the basis of neoliberal ideology. We have shown throughout this paper that this neoliberal move operates through the economisation of authority and the construction of the moral corporation, illustrating these dynamics using the example of Microsoft's "norm entrepreneurship."

The neoliberal push and the ensuing demise of the state are problematic in cyberspace. This is specifically because the economic logic which motivates much of the activity in cyberspace – surveillance capitalism – presents unique

threats to the foundations of our democracies. We therefore urge cyber norm scholarship to be aware of these dynamics and approach any corporate involvement in standard-setting with a critical mind. Moreover, we urge states to reclaim their position as legitimate legislators for the public good, and to unapologetically reject single-minded market logic wherever it threatens democracy, human rights, or the rule of law.

References

Bodhani, Aasha. 2016. *Saudi Arabia strikes deal with Microsoft for Vision 2030.* Online: ITP Media Group. https://www.itp.net/608083-saudi-arabia-strikes-deal-with-microsoft-for-vision-2030.

Boeke, Sergei, and Dennis Broeders. 2018. "The Demilitarisation of Cyber Conflict." *Survival* 60 (November): 73–90. doi:10.1080/00396338.2018.1542804.

Cavelty, Myriam Dunn, and Andreas Wenger. 2020. "Cyber security meets security politics: Complex technology, fragmented politics, and networked science." *Contemporary Security Policy* 41 (1): 5–32. doi:10.1080/13523260.2019.1678855. eprint: https://doi.org/10.1080/13523260.2019.1678855. https://doi.org/10.1080/13523260.2019.1678855.

Eggenschwiler, Jacqueline, and Joanna Kulesza. 2020. "Non-State Actors as Shapers of Customary Standards of Responsible Behavior in Cyberspace," edited by Dennis Broeders and Bibi van den Berg, 245–262. Governing Cyberspace: Behaviour, Power, and Diplomacy. Rowman & Littlefield International.

Fairbank, Nancy Ayer. 2019. "The state of Microsoft?: the role of corporations in international norm creation." *Journal of Cyber Policy* 4 (3): 380–403. doi:10.1080/23738871.2019.1696852. eprint: https://doi.org/10.1080/23738871.2019.1696852. https://doi.org/10.1080/23738871.2019.1696852.

Gill, Stephen. 1995. "The Global Panopticon? The Neoliberal State, Economic Life, and Democratic Surveillance." *Alternatives* 20 (1): 1–49. doi:10.1177/030437549502000101. eprint: https://doi.org/10.1177/030437549502000101. https://doi.org/10.1177/030437549502000101.

Gorwa, Robert, and Anton Peez. 2020. "Big Tech Hits the Diplomatic Circuit: Norm Entrepreneurship, Policy Advocacy, and Microsoft's Cybersecurity Tech Accord," edited by Dennis Broeders and Bibi van den Berg, 263–284. Governing Cyberspace: Behaviour, Power, and Diplomacy. Rowman & Littlefield International.

Guay, Joseph, and Lisa Rudnick. 2017. *What the Digital Geneva Convention means for the future of humanitarian action.* Online: UNHCR. https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/.

Hurel, Louise Marie, and Luisa Cruz Lobato. 2018. "Unpacking cyber norms: private companies as norm entrepreneurs." *Journal of Cyber Policy* 3 (1): 61–76. doi:10.1080/23738871.2018.1467942. eprint: https://doi.org/10.1080/23738871.2018.1467942. https://doi.org/10.1080/23738871.2018.1467942.

———. 2020. "Cyber-Norms Entrepreneurship? Understanding Microsoft's Advocacy on Cybersecurity," edited by Dennis Broeders and Bibi van den Berg, 285–313. Governing Cyberspace: Behaviour, Power, and Diplomacy. Rowman & Littlefield International.

Kalia, Amul. 2016. *With Windows 10, Microsoft Blatantly Disregards User Choice and Privacy: A Deep Dive.* Online: Electronic Frontier Foundation. https://www.eff.org/deeplinks/2016/08/windows-10-microsoft-blatantly-disregards-user-choice-and-privacy-deep-dive.

Koh, Harold Hongju. 2012. "International Law in Cyberspace." *Harvard International Law Journal* 54:1–12. https://digitalcommons.law.yale.edu/fss_papers/4854/.

Mačák, Kubo. 2017. "From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers." *Leiden Journal of International Law* 30 (4): 877–899. doi:10.1017/S0922156517000358.

Nesbit, Jeff. 2017. *Google's true origin partly lies in CIA and NSA research grants for mass surveillance.* Online: Quartz. https://qz.com/1145669/googles-true-origin-partly-lies-in-cia-and-nsa-research-grants-for-mass-surveillance/.

Novet, Jordan. 2020. *Microsoft plans cloud contract push with foreign governments after $10 billion JEDI win.* Online: CNBC. https://www.cnbc.com/2020/08/21/microsoft-plans-cloud-push-with-foreign-governments-after-jedi-win.html.

Schmitt, Michael N. 2012. "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed." *Harvard International Law Journal* 54:13–37. https://harvardilj.org/2012/12/online-articles-online_54_schmitt/.

———, ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge University Press.

Shamir, Ronen. 2010. "Capitalism, Governance, and Authority: The Case of Corporate Social Responsibility." *Annual Review of Law and Social Science* 6 (1): 531–553. doi:10.1146/annurev-lawsocsci-102209-153000. eprint: https://doi.org/10.1146/annurev-lawsocsci-102209-153000. https://doi.org/10.1146/annurev-lawsocsci-102209-153000.

Smith, Brad. 2013a. *Protecting customer data from government snooping.* Online: Official Microsoft Blog. https://blogs.microsoft.com/blog/2013/12/04/protecting-customer-data-from-government-snooping/.

———. 2013b. *Reforming government surveillance.* Online: Official Microsoft Blog. https://blogs.microsoft.com/blog/2013/12/08/reforming-government-surveillance/.

Smith, Brad. 2017. *The need for a Digital Geneva Convention.* Online: Microsoft On The Issues. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

Targett, Ed. 2020. *MOD Hands Microsoft £17 Million Azure Support Contract – Without Competitive Tender.* Online: Computer Business Review. https://www.cbronline.com/news/mod-azure-contract.

United States of America v. Moalin 13-50572, 59 (Court of Appeal, Ninth Circuit 2020).

US Department of Defense. 2019. *Contracts For Oct. 25, 2019.* Online: defense.gov. https://www.defense.gov/Newsroom/Contracts/Contract/Article/1999639/.

Yeung, Karen, and Martin Lodge, eds. 2019. *Algorithmic Regulation.* Oxford University Press. ISBN: 9780198838494.

Zuboff, Shoshana. 2018. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* 1st. Profile Books. ISBN: 9781610395694.