International Journal of Communication 15(2021), 4690–4708 1932–8036/20210005

"Are We Becoming the Kind of Nation That Just Blocks Out All Criticism?": Negotiating the Gap Between Digital Citizenship Education and Young People's Everyday Digital Citizenship Practices in Malaysia

AMELIA JOHNS
University of Technology Sydney, Australia

This study draws on data examining Malaysian official discourses of digital citizenship, as reflected in educational programs targeting young people, and the everyday digital citizenship practices of Malaysian-Chinese youth in Kuala Lumpur. The study examines two programs and their alignment with laws censoring contentious digital speech and content. This is contextualized and analyzed via semi-structured interviews with stakeholders from government and industry, and ethnographic interviews with *N* = 29 Malaysian-Chinese young people (aged 18–24). The analysis provides insight into the content of digital citizenship programs, which seek to responsibilize young people to police their own online speech, while encouraging them to engage in lateral surveillance of their peers. I argue that digital citizenship is part of a surveillance assemblage that had chilling effects on youth political expression in the lead up to the 2018 General Election. Nonetheless, interviews with young people also showed them engaging in digital acts of resistance. In this study, I analyze one of these acts—platform-switching from social media sites to encrypted chat on WhatsApp.

Keywords: WhatsApp, surveillance, encryption, lateral surveillance, digital activism, resistance

In 2018, Malaysia's 14th General election (GE14) seemed poised to usher in a new era for Malaysian politics, with ruling coalition, *Barisan Nasional* (BN), voted out for the first time since Malaysian Independence. The victory of the opposition party was led by a youth voter surge, with young people, who make up roughly 40% of voters, being hailed the "kingmaker" in GE14 (Chinnasamy & Azmi, 2018, p. 125).

This followed the 2013 election (GE13) where BN lost the popular vote for the first time, providing momentum to activists seeking political change and prompting calls for the citizenry to reclaim Malaysian democracy from a semi-authoritarian government. Attention on themes of political corruption escalated in the lead up to GE14, with a much publicized scandal involving Prime Minister Najib Razak—who was accused, and eventually found guilty, of siphoning at least $10 million USD of taxpayer funds into his personal bank account (British Broadcasting Corporation [BBC], 2020)—providing further impetus. Growing objections to Najib-era politics also centered on the government's use of the Sedition Act (1948) and section 211 and 233

Amelia Johns: Amelia.Johns@uts.edu.au
Date submitted: 2020-12-15

of the Communications and Multimedia Act, or CMA (1998; Article 19, 2017), to target and arrest citizens expressing views critical of government on social media (Johns & Cheong, 2019; Lim, 2016; Mohd Sani, Ahmad, & Wahid, 2016). This was perceived to break a contract forged between the government and citizens in the late 1990s, that the Internet would remain uncensored. This guarantee accompanied public investment in broadband initiatives to secure Malaysia as a frontrunner in an era of digital modernity (Bahfen, 2009; Lim 2016). The shattering of this contract, alongside a belief that it was opposition voices who were silenced by the suppression laws, caused public unrest and "chilling effects" in the lead up to GE14 (Johns & Cheong, 2019).

Mirroring this increase in more restrictive laws policing digital content and speech, Malaysia's digital citizenship (DC) education programs took a turn toward suppression rather than empowerment after GE13. But there are some indications this began even earlier, with the launch of the CyberSafe in Schools program in 2010 (UNESCO, 2015). Arising from a partnership between CyberSecurity Malaysia and the Ministry of Education, and later joined by Digi, a Malaysian Telecommunications company, programs launched under this framework focused on educating young people to prevent online harms such as scams and phishing. Misuse of digital media was also addressed with programs focused on cyberbullying, harassment, and stalking. However, very little mention was made of social media's capacity to empower young people to understand their rights as citizens.

In 2012, the Malaysian Multimedia and Communication Commission (MCMC) launched a school-based DC program, *Klik Dengan Bijak* (MCMC, 2020a; UNESCO, 2015). This program saw MCMC partner with UNICEF, whose efforts to advance regional DC programs via its Voices of Youth project (Third, Bellerose, Dawkins, Keltie, & Pihl, 2014) led to a new focus on youth empowerment and children's digital rights (Livingstone & Third, 2017). Nonetheless, the outcomes were limited by MCMC's hesitation, in some cases, to support the connection of digital citizenship to the UN Convention on the Rights of the Child (CRC), given sensitivities around young people's freedom of expression in the Malaysian context.

In this article, I will examine how these tensions open a gap between formal DC educational programs—which align with laws curbing contentious digital speech and misuse, on the one hand; and young people's everyday practices of digital citizenship that, as this study highlights, includes actions to resist and subvert government monitoring and surveillance, and create safe spaces for young people to engage more freely in public discussion. Nonetheless, the article also examines the limitations of these acts of resistance by arguing that DC educational programs have normalized an understanding that digital communication presents dangers that young people must protect themselves from by participating in "lateral surveillance" (Andrejevic, 2005). This leads even the supposedly safe spaces of WhatsApp groups to become monitored spaces. The analysis will include data from interviews with government stakeholders, and ethnographic observation and interviews with *N* = 29 Malaysian-Chinese youth, hailing from Malaysia's largest ethnic minority group.

Young People, the Malaysian Internet, and Connective Action

At the time of GE14, 70% of Malaysians had access to the Internet (MCMC, 2018). The ubiquity of smartphone access and generous mobile data plans made communication apps the most popular social media in 2018 (MCMC, 2018; Tapsell, 2018), with WhatsApp leading a crowded marketplace (98.1% of Internet users). This was closely followed by Facebook, which remained the most popular social networking service (97.3% of users). Internet and smartphone usage was skewed toward young people with 20–24-year-olds being the largest user-group in the country (MCMC, 2018). Observers of GE13 identified young, urban people as a growing force in Malaysian electoral politics, with voter participation increasing from 76% to 85% (Weiss, 2013); a growth that was attributed to social media participation. This was further addressed in the context of the electoral defeat of BN in GE14, with Tapsell (2018) discussing the growing reach of smartphone usage. With smartphones becoming "more affordable for middle- and lower class Malaysians" (Tapsell, 2018, pp. 12–15), applications like WhatsApp, Tapsell argued, became a "weapon of the weak," with the app being used to engage in political chat to subvert "authoritarian rule" (p. 11).

Some scholars have explained the youth voter surge by connecting young people's social media use with a widening of political repertories of action (Mohd Hed & Grasso, 2020, p. 766). Not that this trend is a unique outcome of the introduction of social media in Malaysia; the use of the Internet as a tool to counter government suppression of critical news reportage precedes the introduction of social media. The *Reformasi* movement, which swept across Malaysia and Indonesia in the late 1990s, was the first Internet-enabled movement to harness and mobilize citizen anger at government corruption and creeping authoritarianism. *Reformasi* blogs, websites, and independent online news sites overcame "structural, organizational and resource disadvantage" (Khoo, 2016, p. 73) for opposition parties and activists, offering them a chance to gain legitimacy, a voice, and, eventually, electoral power (Johns & Cheong, 2019; Lim, 2016; Weiss, 2013).

The shift to social media has likewise introduced structural reorderings, including the decentering of party politics as the dominant source of political authority (Khoo, 2016; Lim, 2016; Weiss 2013) with "cleavage-crossing" and "issue-oriented" mobilization (Weiss, 2013, p. 605), fostering new collective identities that bridge divisions associated with ethnically aligned political parties. These shifts strongly reflect arguments claiming social media has shifted political engagement away from collective action toward "connective action" (Bennett & Segerberg, 2012), which Bennett and Segerberg define as an historical break from participation in centralized and hierarchical "organizations or membership groups" that use their resources to persuade people to identify with a collective "we" (Bennett & Segerberg, 2012, p. 748). According to logics of connective action, this is replaced with participation in "large, fluid networks" that operate through the organization of social media and "personalized action frames" (Bennett & Segerberg, 2012, p. 748). The new connective logic is one that appeals to young Malaysians seeking a move beyond the old political establishment and ethnically aligned political membership groups (Bahfen, 2009; Lim, 2016); a view strongly held by ethnic minority youth in Malaysia, for whom the old-style politics are seen to keep minorities in their place and to reassert the ruling regime's political dominance (Harris & Han, 2020; Koh, 2017).

Digital Citizenship, "Youth at Risk," and the Control Paradigm

Although scholarship focused on Malaysia continues to equate social media participation with new forms of connective action in a post-*Reformasi* period, scholars are beginning to note more restrictive Internet laws and manipulation of social media publics to suppress free speech (Cheong, 2021; Sinpeng &

Tapsell, 2020). This is reflected in DC educational programs that, from the outset, have bypassed recognizing the importance of social media for social inclusion and democratic expression, and, instead, have discursively positioned everyday digital media use as risky, prompting calls for more monitoring and surveillance of children and young people's Internet and social media use.

While state efforts to protect young people from online risks have tended to be top-down, DC programs are seen as an important next step to mold young people into regulating online environments themselves. In *Klik Dengan Bijak* (MCMC, 2020a), for example, young people are positioned less as victims, in need of protection, and more as "citizens-in-making" (Harris, 2013, p. 27), for whom responsible online behavior needs to be cultivated through education. This is reflected in the downloadable resources available on the website, with two resources—"Know the Law" (MCMC, 2020b) and "Self-Regulation" (MCMC, 2020c)—providing insight into how digital citizenship is conceptualized by policymakers. These resources emphasize obedience to the law as opposed to young people learning about their rights. In "Know the Law," citizens are provided with a list of offenses related to digital speech, with the Sedition Act (1948) at the top of the list (MCMC, 2020b, p. 1). In "Self-Regulation," citizens are directed to a list of qualities defining how to "be a responsible citizen" and answering the question "why self-regulate?" (MCMC, 2020c, p. 1). The main message is that in a world where authorities cannot monitor all digital interactions online, digital citizens must "actively report and sanction offensive content, in order to safeguard their community" (MCMC, 2020c, p. 1).

These conceptualizations of digital citizenship connect with much of the literature in the UK, Australia, and the United States (Isin & Ruppert, 2015; Livingstone & Bulger, 2014; McCosker, 2015), all of which have strongly influenced policy development in Malaysia and across the region. Third, Collin, Walsh, and Black (2019) outline the policy challenges around children and young people's digital rights discourses globally by arguing that governments around the world have focused too much on risk and protection, prioritising a "control paradigm" (pp. 44–45). The "control paradigm" is defined by Third and colleagues (2019) as "a constellation of policies, practices and mainstream media representations [. . .] that draw upon deficit framings of youth-at-risk [. . .] the result is a more-than-usual exercise of control rendered possible by 'technologies of suspicion' and 'pedagogies of surveillance'" (pp. 44–45).

McCosker (2015) speaks of how DC education encourages young citizens to participate in regulating online sociality through "appropriate use" (p. 21) while their own conduct is regulated through parental and government controls. He analyzes how these forms of control are often more closely connected to state apparatuses and domains of security, on closer investigation, than young people's rights to protection and safety. For McCosker (2015), online safety is determined by three layers of governance that constitute appropriate technology use: "laws and state regulation [. . .] platform controls in the form of technical codes and monitoring and flagging tools, and the application of norms through educational programs" (p. 21). This raft of policy interventions centers on the concept of the young person as a deficit citizen, needing to be guided toward an ideal mode of participation. In terms of what this participation looks like, he argues there is a "persistent idea . . . that the 'social' should be rational, conflict and risk free" (McCosker, 2015, p. 24) smoothing over any eruptions of "the political" (Mouffe, 2011) that might disrupt the smooth functioning of state power.

This understanding, that digital citizenship pedagogies and education are aimed more at maintaining security and protecting the status quo, rather than empowering youth voices, connects the digital citizenship scholarship with surveillance studies. Surveillance studies have long focused on the way that surveillance technologies serve as a central technique of government to produce ideal citizen-subjects (Hintz, Dencik, & Wahl-Jorgensen, 2019; Isin & Ruppert, 2015) who internalize the knowledge that they are being watched by authorities through all manner of institutional, architectural, electronic, and digital modes of monitoring, recording, and datafying their activities. This produces a self-surveillant or self-monitoring subject who performs an acceptable citizenship for governing authorities out of fear of punishment, without the need for such spectacles of punishment. This strongly evokes Michel Foucault's metaphor of the panopticon as a form of hands-off social control where technologies enabling the "few to watch the many" presents a normalizing gaze that molds "self-controlling subjects fitted for democratic capitalist societies" (Lyon, 2006, p. 42). Nonetheless, in an era where datafication of our everyday lives has expanded exponentially beyond the controlling gaze of the few (Hintz et al., 2019; Lyon, 2006), the metaphor of panoptic power has gradually been replaced by other concepts.

From Self-Monitoring Subjects to Lateral Surveillance— Tapping Into Connective Action?

One such concept that has emerged from the digital turn in surveillance studies is the concept of lateral surveillance. Andrejevic (2005) uses this concept to refer to the way social media platforms have created new logics that equate watching and monitoring peers with aspects of enjoyment and desire. But despite this entanglement of surveillance and enjoyment, Andrejevic (2005) regards these opportunities to engage in peer-surveillance in a "networked communication environment" (Andrejevic, 2005, p. 482) as having a strong alignment with neoliberal logics of responsibilization. As far as this logic goes, narratives about the proliferation of risks in the contemporary era and the impossibility that risks can be sufficiently managed by governments and other institutions, have led to revised techniques of government that offload the surveillance practices of the state onto individuals. In this way, citizens become enlisted to "take on some of the responsibilities not just of monitoring themselves, but of keeping track of one another":

> Internalizing the gaze—in an era of governance in terms of risk—comes to mean not just turning it upon oneself (in anticipation of the possibility of being watched), but also directing it outwards toward others (as if to fill in the gaps of the big Other's gaze, to realize this gaze in a skeptical era), in the name of responsibility towards oneself. (Andrejevic, 2005, p. 485)

The transformation of the self-monitoring citizen into a citizen engaged in lateral surveillance is continuous with how digital media scholars discuss the entanglement of state surveillance with the surveillance logics of private digital media platforms. As Hintz and associates (2019) stress, platforms harvesting our personal data for profit-driven ventures, and citizens willingly participating by making personal information public, has come to be accepted as "part and parcel of everyday life" (p. 5). These transformations have been noted in the Southeast Asian context—with arguments that social media is a democratizing force or a "liberation technology" (Sinpeng & Tapsell, 2020, p. 2) being replaced with a view that social media and its surveillance logics are being weaponized to reinforce authoritarian arrangements of power, enabling states to monitor and police citizens and publics (Hintz et al., 2019; Sinpeng & Tapsell, 2020). Drawing on Andrejevic's (2005) concept of lateral surveillance, research has documented how citizens have also been encouraged by governments to engage in peer surveillance to supplement the state's top-down surveillance activities (Jiow & Morales, 2015). These operations mobilize and weaponize a connected citizenry, inverting the arguments previously mentioned that consider how networked social media introduces new forms of "connective" political agency, identity, and action. Lyon (2016) acknowledges that most social media occupy a "gray zone," where participatory cultures that enhance the voices of the marginalized intersect with top-down practices of surveillance and bottom-up practices of lateral surveillance that enrol watchful citizens into larger "surveillance assemblages" (Hintz et al., 2019, p. 5.)

Universal or Culturally Specific Modes of Governing Young People's Social Media Use?

Notwithstanding similarities among Malaysian, UK, and Australian digital citizenship discourses and programs, Ong (1999) and Lim and Soriano (2016) argue that scholars must challenge the tendency to frame digital cultures and participation norms according to Eurocentric concepts and knowledge.

These authors refer to the influence that "Asian values," as well as colonial era legacies, have had on young people's relationship to citizenship in South East Asia and other Asian countries (Koh, 2017; Ong, 1999). In relation to the former, Asian values refer to the influence of Confucianism, Islam, and a range of cultural and religious influences on Asian identities. These influences are argued to instil a greater emphasis on familial piety and loyalty and respect for authority, leading to a foregoing of personal freedom and individualism. This claim was most famously argued by former Malaysian Prime Minister Mahathir bin Mohamed, in the 1990s, to suggest human rights are culturally relative and privilege Western style values of individualism that don't align with Asian values (Sergeant, 2018). Nonetheless, for Ong (1999), this is related more so to an argument for cosmopolitanism and "flexible citizenship," whereby Chinese cultural tradition is seen to shape a sojourner citizen subjectivity, reluctant to engage publicly in politically sensitive topics that might jeopardize the advancement of personal reputation and family standing.

In addition, Bahfen (2009) argues that because the Internet and digital technologies were introduced into S.E. Asian countries at a time of growing public sentiments that colonial era laws and legacies were protecting the political interests of the few—leading to calls for reform (*Reformasi*)—that these technologies were, at the outset, invested with a sense of civil society renewal, an end of the old oligarchies and, in Malaysia's case, a "modern Malaysian" identity. Part of the branding of the "new Malaysia" included embracing Malaysia's multiethnic heritage (comprising Malay, Chinese, Indian ethnic groups, and Indigenous groups, such as the Orang Asli) and embracing a social code built around constitutionally enshrined principles of religious pluralism and intercultural harmony (Harris & Han, 2020).

These implicit citizenship norms have become central to DC educational policy and programs in Malaysia, with the *Rukun Negara* being enshrined as the ethical framework for "good" digital citizenship and positive social interaction online, since 2012. The *Rukun Negara*, which lays out national principles for Malaysians, was introduced in the 1970s as a response to racial tensions and hostilities that culminated in the 1969 race riots between ethnic Malay and Chinese citizens. The *Rukun Negara* was introduced to foster interracial harmony through the shaping of universal Malaysian norms and values based around religious values, loyalty to king and country, observance of rule of law, courtesy, and morality. It is recited in Malaysian schools and shapes normative social interaction, with online conflict (including some forms of political contestation) frequently being condemned by state and civil society as a figure of the bad society. In this context, the use of sedition laws and the CMA to close down "offensive" or contentious speech, often draws on the race riots as a warning, with the *Rukun Negara* functioning as an antidote to political violence.

In this analysis, I will examine how these frameworks and imaginaries, together with the "control paradigm" discussed in the previous section, apply to DC programs and discourses, as reflected in policymaker interviews. I will also consider gaps between these discourses and the everyday digital citizenship practices of Malaysian-Chinese young people in Kuala Lumpur, Malaysia. In particular, the study will address the questions: Is there a perceived gap between government visions and policy and young people's aspirations as digital citizens? How is this resolved in practice? And how might DC programs be broadened to accommodate complex claims?

Study Overview and Methods

This article draws on data and findings from a study comparing formal DC policies and educational programs in Malaysia and the everyday digital citizenship practices of Malaysian-Chinese youth residing in Kuala Lumpur. The purpose of the study was to understand how DC educational programs inform the everyday civic and political practices of young people from Malaysia's ethnic Chinese community, and whether participants experienced any gaps between the objectives of these programs and their own everyday digital civic and political practices and aspirations.

The sample for this study consisted of *N* = 29 youth participants, aged 18–24, who were recruited using targeted as well as convenience sampling, and *N* = 6 policymakers who were recruited based on a desk review of Malaysia's DC policies and programs. In these interviews, participants were asked to identify (a) the content of their programs, (b) what kind of digital citizens they saw their programs fostering, and (c) whether these goals and aspirations accommodated the everyday civic and political practices and expressions of young people.

To recruit youth participants, advertisements were placed in known activist social media (including by invitation to closed WhatsApp groups), as well as student association Facebook groups and social media. In 2016, the first phase of field research, semi-structured interviews of roughly 60-minute durations were undertaken with *n* = 21 informants using techniques designed to open up interviews beyond traditional Q and A format (i.e., the research team used video and screen capture to elicit spontaneous responses from participants as they scrolled through their feeds; Pink et al., 2016; Robards, 2013). This was followed in 2018 by a second field trip, which included follow-up interviews with *n* = 4 participants from the 2016 cohort. Interviews were also conducted with a further *n* = 8 participants. The interviews focused on young people's everyday digital practices and the composition of their social networks. Further questions asked about their levels of political and civic engagement and how they expressed themselves as digital citizens, though it should be noted that participants did not register strong familiarity with DC programs and were more familiar with laws limiting digital speech.

Interviews were conducted in English and thematically coded and analyzed using Nvivo. Pseudonyms have been used in the article instead of real names. Coding followed the interview themes but also included open coding, to identify themes that challenged or didn’t easily fit within the original coding scheme.

Limitations

In keeping with an ethnographic approach, the sampling method was not intended to achieve representativeness. I acknowledge that this introduces potential bias in the sampling and limits the study findings.

Findings

Digital Citizenship Educational Programs and the Control Paradigm

Mr. Wan of CyberSecurity Malaysia identified oversharing sensitive information on social media and not protecting passwords as major challenges that were addressed in DC programs, with a lack of awareness and technical competency leading young people to fall victim to cybercrimes, scams, and sexual exploitation. But he also identified behaviors that produce conflict, and “bad words” being uttered about different races and religions—what he called “seditious statement”—as a vexious issue. This was addressed in DC programs by encouraging young people to limit oversharing on sensitive topics, often with a warning of possible reputation damage and legal action.

This strategy of responsibilizing young people to manage their own digital identity, reputation, and safety fits with Third and colleagues’ (2019) understanding of the control paradigm and McCosker’s (2015) three-layered model of digital citizenship governance. Each of these emphasize the entanglement of regulatory codes and laws, and the use of educational programs to encourage the not-yet-citizen to become self-regulating. Mr. Wan explicitly stated that self-regulation was a preferential outcome of DC programs in Malaysia:

> If you ask me, education is the best way to get all the young people to self-control themself [sic.]. So you don’t need to have law to control them. It’s not just about purely technical. It’s also about the non-technical . . . That’s the best way, to self-regulate. I think even regulator will love that, isn’t it? Less job for them. (Mr. Wan)

Mr. Wan’s humor reflects shifts in government discourses concerning young people’s digital media use, with top-down forms of control being supported and extended via promotion of neoliberal techniques of government that shift responsibility for regulating online sociality onto young people.

Despite using the concept of citizenship to describe these programs—implying a balance is struck between raising awareness of citizen rights and responsibilities online—the focus on user rights was largely absent. Where rights were mentioned, the focus usually fell on provision (digital access and inclusion) and privacy rights. There was little-to-no discussion about social media advancing opportunities for young people to advocate for their rights in a democracy, despite some young people interviewed in the study becoming old enough to vote in 2018.

Adam, a stakeholder from Digi, a Malaysian Telecommunications company involved in the CyberSafe in Schools program, did stress that as part of the company's human rights due diligence,[1] he had introduced a program advocating for minority youth inclusion and participation. Partnering with UNICEF, Digi provided tablets to Indigenous youth in Sabah with the aim of assisting them to plot out local impacts of climate change. However, there were limits when dealing with issues considered "too sensitive" given Digi's status as a corporate partner:

> We are also a bit more careful. Because although we bring up the rights of the Indigenous [. . .] a lot of these youths are also championing local issues like building of the dam in Sabah which sometimes is sensitive for us because we fall under the ministry's purview [. . .] it's a balancing act. (Adam)

This feeling of being limited in pushing too far to highlight young people's rights of expression was further explained by Mr. Wan (Cybersecurity Malaysia). Mr. Wan claimed that "free speech" was limited in Malaysia owing to a communitarian social structure that contradicted "Western" rights discourses. In this instance, he implicitly references the Asian values debate, arguing against the efforts of UN agencies and not-for-profits to empower young people's voices and participation through DC programs:

> In the context of western countries there's issue of freedom of expression, so you can say anything. But in countries like Malaysia, there is laws that need to be abided to. There are issues that you cannot just say anything that could create tension. Called seditious statement. (Mr. Wan)

Although hate speech and libel laws also exist in other nations and are considered an important limit to free speech, fears that the Sedition Act and CMA had been weaponized to arrest and charge activists and citizens who criticize government was growing in Malaysia at the time the interviews took place. Billy, a campaign manager for *Bersih*, said with reference to the CMA:

> After the 2013 general elections there was a conscious strategy to go after people who are on social media saying things . . . There is also an increasing trend now to use the Multimedia Communications Act because the act says if you're posting and what you've said has offended somebody—I'm serious, it says offended. So, that's really so broad and that's the basis of a criminal offense. (Billy)

This view was supported by academic and human rights organizations who felt that the vagueness of legal terminology around what constitutes "offensive speech" in the CMA was designed to make citizens self-aware of possible legal repercussions when expressing a political opinion (Article 19, 2017; Lim, 2016;

[1] This refers to a National Labor Framework set up to comply with Free Trade Agreements signed with other ASEAN states, and that follow UN "Guiding Principles on Business and Human Rights" (UNGPs).

Mohd Sani et al., 2016). Nonetheless, Ms. Tan, from MCMC, felt this criticism was not a reflection of the reality. She asserted that the laws were unambiguous, and the regulator had very clear guidelines:

> Well the thing is we are guided by the content code. So they do have guidance in terms of what is construed as being obscene [. . .] Our cases are about obscene animes[2] being sold to children. Our cases are also about very bad words being uttered against royalty. Of course there are going to be differences in terms of interpretations. (Ms. Tan)

Though the regulator had also begun looking at the growing problem of misinformation by encouraging young people to: "analyze information, and also understand agendas behind news reporting," there is some perceived conflict in educating young people to increase critical thinking, while at the same time censoring online speech (including speech critical of government).

A clear part of the responsibilization strategy expressed by stakeholders was encouraging citizens to police online discourse through formal complaints procedures, which were required (by law) to trigger prosecution and enforcement. To inform citizens of how to lodge a complaint, MCMC found outreach programs like *Klik Dengan Bijak* to be necessary in creating social conditions for digital citizens to act in the informant role:

> It's also about public responsibility meaning you have to stand up for what's bad in terms of pushing it through the legislative system because we can't do it, we can't act as the complainant . . . So that's also part of being a good digital citizen. (Ms. Tan)

The transformation of the self-surveillant digital citizen into a citizen engaged in surveillance of others, and the idealization of this citizen subjectivity in policymaker accounts of "good digital citizenship" strongly suggests the prioritization of "lateral surveillance" (Andrejevic, 2005) as a technique to regulate social media environments.

Paying Attention to Young People's Platform Specific Cultures and Literacies

Facebook's "Default Publicness" and Surveillant Citizenship

For youth participants, mobile phones and social media connected them to an ecosystem of friend and family connections, status updates, popular entertainment, and news. Political activism and political engagement was not often a primary focus. However, for young people who were voting for the first time in GE14, platforms like Facebook, WhatsApp, and Instagram were becoming more frequently used to express political opinions and to mobilize peers to vote.

Of the N = 29 youth participants who participated in the study, all had Facebook and used it to manage contacts and social calendars, read status updates, follow news organizations, and join like-minded groups. Language use was predominantly in English and Bahasa Melayu (BM), with only n = 3 participants

[2] This refers to anime and manga cartoons which depict pornographic imagery.

using Mandarin mixed with English. But despite the wide use of Facebook, engagement on the platform was often quite passive, with only a few participants posting content regularly. This was because participants tended to have more diverse contacts on Facebook than on their other social media accounts (including close friends and family, extended family, university contacts, professional contacts, clients, and more.) This would often mean that discussions around personal or contentious topics were avoided to protect personal reputation. There was some suggestion that posting on political or contentious issues was not safe owing to who was watching. For example, Verona advised, "I don't post anything on there (Facebook). And if work people try to add me I will deny them. It can become a bit of a surveillance tool," while Monica added, "typically I don't comment on public posts on Facebook, I only read through most of the stuff. I sometimes don't really feel entirely safe to say what I want to say." Rhys added that this was "because there are always people watching even if you've set your settings to private or only friends can see."

This reluctance to post contentious or political opinions was related to platform specific cultures and literacies, with Facebook being identified as an important platform for maintaining social connections and projecting an acceptable self-image to the diverse contacts in your network, but also "a bit of a surveillance tool." One participant regarded it to be "like a resume" where you put your best face forward, but where everyday thoughts, beliefs, frustrations, and concerns remain "in the background." If the rules were breached, and participants posted about contentious topics, Facebook quickly became a toxic space where bullying, harassment, and trolling of posts was common. As Cassie, a journalist whose job required her to report on social and political developments in Malaysia, disclosed, she no longer posted her political views in status updates after she had previously been harassed for her views on Malaysian race politics, feminist and LGBTIQ+ issues:

> I did a post on gaming once—it was Assassin's Creed—and I said they didn't have proper female characters . . . It was just from one guy who was calling me a crazy feminist who doesn't know anything she's talking about in terms of Assassin's Creed—or gaming in general. And I was wrong because of this and this and this and this. And then I engaged and it kind of just escalated from there. (Cassie)

These descriptions confirm scholarly work on Facebook's "default publicness" (Cho, 2019). Cho argues that Facebook's design bias, which makes the "communication archive as readable and traversable as possible," while "broadcasting one's actions to one's networks without one's knowledge" (Cho, 2019, p. 3184) makes it an unsafe space for women, LGBTIQ+, and other minority youth. This is because it is difficult for users to have full control over the visibility of posts, who sees them, and who responds.

The fear of possible harassment and retaliation from close contacts or friends of contacts when discussing sensitive topics was identified by a further *n* = 7 participants. Anita and Arlene claimed that the tendency for close contacts to police political opinion expression also came from social conditioning from within their culture and community. As Anita argued, there was a reluctance to speak out openly if it might lead to conflict: "I think Malaysian Chinese they have very high tolerance level. It's not to say we don't feel angry about things but this is how we have been (conditioned) for over 50 years."

The social conditioning to be courteous and polite online aligns with Ong (1999) and Lim and Soriano's (2016) arguments, that to be polite and not to engage in political or contentious speech was often culturally prescribed. But significantly, this was also framed by participants with reference to a political, legal, and educational system that strategically silenced young people's voices, limiting critical thinking and speech that might challenge the status quo.

Monica also experienced bullying on social media for expressing a view about women's rights, and this made her "shy" to post or comment about political issues again. She argued that some of this reluctance was because of social conditioning from school:

> It comes from community and even in our education system itself. There are a lot of things that are, like it's specifically said that we can't talk about race, and in Malaysia, with politics, I think everything comes back to race, so it becomes very taboo to talk about a lot of things. (Monica)

These responses provide insight on the manner in which education on digital use and political speech stresses the importance of minimizing conflict and harm, meaning politeness becomes an ideal expression of citizenship; and conflict its antithesis.

Sedition Laws and State Surveillance of Everyday Political Chat

But despite the feeling of being constrained by cultural and social norms, participants also expressed a reluctance to speak up on Facebook owing to the threat of the sedition laws and the CMA. Ben, a Facebook page admin for a political think tank, spoke about his friendship groups on social media, some of whom posted political opinion about sensitive topics such as disagreement with the "Islamisation" of the public sphere. He explained his own reluctance to do so out of fear that speaking up might subject him to the Sedition Act, and possible reputation damage:

> When you're a minority in Malaysia, and you say things that are against the current status quo, it does endanger you because you just get sidelined into this one big grey group that is racist, that is questioning the status quo . . . it [Sedition Act] is omnipresent, always in the background waiting for you to make some sort of statement that you can get hauled away for. (Ben)

This, and earlier discussions about surveillance and reputation management on Facebook connect with research identifying profile and newsfeed curation on the platform as a negotiation of social media "publicness" (Baym & boyd, 2012) that is mutually shaped by platform affordances, social practices of self-presentation, and audience management. In discussing how social media require different presentations of self, Marwick and boyd (2010) draw on Erving Goffman's metaphor of the stage as a social setting where the spatial architectures of "frontstage" and "backstage" account for different performances and presentations of self (Marwick & boyd, 2010, p. 123.) This is especially so for social networking sites such as Facebook, where the architectures of the platform that "collapse multiple contexts and bring together commonly distinct audiences" (Marwick & boyd, 2010, p. 115) lead to hyperawareness of possible unintended consequences of disclosing personal information to the wrong audience.

In the lead up to GE14, there was a sense that anything one said on Facebook and Twitter about politics could be defined as seditious. For one participant, an auditor, who had signed a confidentiality agreement with her employer barring her from making public comment about political issues on social media, the vagueness of what was considered seditious led to feelings of frustration:

> There are things that we should be made aware of like maybe the rules and regulations [of the Sedition Act and CMA] . . . maybe we need more explanation and information about it . . . and I guess sometimes when all these acts come about it just feels so limiting to us because it's like, it's just like the government is so insecure . . . Are we becoming the kind of nation that just blocks out all criticism? Because we weren't like that, then you started implementing all these things. (Kathy)

On the other hand, Clare, an intern for a political candidate in GE14, disclosed that, during the campaign, she felt pressure to use her personal social media to publicize the candidate's campaign, an expectation that led her to become hesitant to post any personal political views in case it should lead to embarrassment or backlash from the candidate, but also owing to fears that the Sedition Act or CMA might be used against her:

> Ever since interning with [name removed] and always going back to his office, my pictures will always be on his Facebook page and I was like oh no it will be in sight, so I think I was shy or hesitant to want to go public with a lot of things [. . .] I was very aware of what happens when you speak against the government at that point in time [. . .] So, then because of that, it made me self-censor. (Clare)

Platform-Switching to WhatsApp and New Fears of Lateral Surveillance

Notwithstanding fears about posting political or contentious content on the social media "frontstage" (Marwick & boyd, 2010, p. 123), these platforms were still used by youth activists to mobilize their networks to vote in the lead up to GE14. But for more risk-averse participants, fear of the Sedition Act and CMA drove them to either withdraw, or it led them to platform-switch to WhatsApp and Telegram. Both platforms were considered safe spaces to discuss politics and engage in activism, with the default end-to-end encryption of WhatsApp allowing a strategic retreat to the social media "backstage" (Johns, 2020; Treré, 2015).

"Switching," as Haggerty and Ericson (2006) claim, is one of the 11 general strategies of surveillance resistance (p. 20), which enables the "default publicness" (Cho, 2019) of platforms like Facebook and associated techniques of surveillance to be "resisted or subverted" (Haggerty & Ericson, 2006, p. 20). Platform-switching implies "familiarity with the protocols and optics of a particular surveillance system," (Haggerty & Ericson, 2006, p. 20) and also intimate knowledge of the architectures and affordances of alternative media. To this end, Hintz and associates (2019) have described contemporary methods of "data activism" with activists and ordinary citizens subverting or resisting the surveillance gaze of the state through use of communication methods "strengthened by encryption" (p. 129).

Of participants interviewed, roughly half of ordinary users, and all of the activists we spoke to, expressed a belief that WhatsApp was a safe channel for them to engage in political discussion. This was emphasized by Billy, a campaigner with *Bersih*, who advised that WhatsApp was their go-to to platform to broadcast campaign information: "If we need to disseminate information, or mobilize people for certain things, it's just a matter of mass communicating through WhatsApp." Rhys, a law student, emphasized a sense of safety associated with the WhatsApp backstage that was not afforded by Facebook: "In terms of my engagement, it's always mainly been WhatsApp. I think because it was somewhat of a safer, safe for me in that sense to discuss politics, rather than discussing it publicly on Facebook." Julian linked this feeling of safety to the encryption affordance:

> When WhatsApp came in they were all saying, "Oh Facebook's going to buy WhatsApp, they're going to suck in our phone numbers" . . . our worst fears have not come to pass and they've also introduced encryption. So we are at least safe from the Government, but not necessary from Facebook. (Julian, activist)

For activists who were involved in campaigns to abolish the Sedition Act or who were otherwise protesting government arrests of activists and politicians under either the CMA or Sedition Act, WhatsApp and Telegram were preferred platforms, although some activists invested more trust in the security credentials of Telegram:

> Most of my activist friends are on WhatsApp . . . I already tell them Telegram is better, more secure, but a lot of them refuse to turn to Telegram because I believe it's also affected by the crowd . . . WhatsApp if more famous here (Hai Yang)

This comment speaks to the market dominance of WhatsApp in the Malaysian context that, despite owner, Facebook's, poor record relating to privacy and security, is often preferred over rivals such as Telegram.

From the interview data, it is easy to identify a feeling that posting certain political opinions on more public-facing social media was not only likely to lead to hostile and polarizing debates but that it also had the potential to trigger legal actions. This led many users to platform-switch to WhatsApp, to evade the surveillance capabilities of the Malaysian government. But despite this, participants also spoke of highly publicized events that made them limit their trust in encrypted chat platforms, such as one case where a 78-year-old "uncle" was arrested for posting a photo that offended the prime minister in a WhatsApp group. This and other incidents led participants to suspect "spies" were in their WhatsApp chats. As Billy mentioned, "We work on the assumption that whatever we are saying on WhatsApp is under surveillance, so, based on that, then, we also evaluate what kind of information can be shared through WhatsApp or not." Anita also felt hesitant to post political opinions on a WhatsApp group chat for fears the conversation might be recorded by law enforcement: "I wouldn't give it in WhatsApp or any recorded setting . . . There are news that police tend to catch people who are spreading the rumours on WhatsApp." Participants understood WhatsApp affordances, like being able to screengrab and share conversations, as problematic, eroding the benefits of encryption—"I mean you can have a fear of like, what if somebody screenshots this and sends it to someone else."

Perhaps the most telling reflection on the limitations of WhatsApp's end-to-end encryption came from Julian, who claimed after GE13:

> Of course the technology is only as strong as the human link. So there were cases that came up in the year previous to the election [GE14] where there were student groups that were affected where the government would simply insert one of their agents into the group . . . You have no protection from the encryption at that point.

Conclusion

The construction of a surveillant-digital-citizenship model—as reflected in stakeholder and youth accounts presented in this study—provides insight into how technologies and pedagogies of surveillance are integral to how DC programs are imagined and operationalized in Malaysia. In particular, this was found to have created a self-regulating digital citizen, where fears of disclosure, reputation damage, and even arrest under the Sedition Act and CMA silenced or chilled speech critical of government. This was emphasized in interviews with youth participants in the study, who perceived that efforts to shape self-disciplining, self-policing digital citizens, as an outcome of social conditioning and educational interventions, dampened their ability to express themselves freely online. The emphasis on surveillant digital citizenship was also extended out through the media ecosystem (including encrypted chat) via government efforts to promote lateral surveillance among the citizenry.

In terms of how participants themselves conceptualized online safety and digital citizenship, most supported some principles instilled in DC programs, as reflected in their decisions to be mindful of the "publicness" of their posts and to use tactics such as platform-switching to manage privacy, protect personal reputation, and create safe digital environments. But ironically, this strategy was predominantly used to protect themselves from government surveillance rather than the cyber-criminal, cyber-bully, stalker, or predator, as imagined in DC programs. For participants, the merging of state and lateral surveillance into a singular "surveillant assemblage" (Haggerty & Ericson, 2006) made them wary to engage in political discussion for fear that saying the wrong thing might lead to arrest, even in encrypted chats.

Nonetheless, the suppression of speech critical of government did not lead to positive outcomes for the ruling regime in GE14, with BN losing power. This was led by a surge in the youth vote, as argued by Chinnasamy and Azmi (2018). Findings also show that WhatsApp—despite being leaky, owing to lateral surveillance—was still an important platform for youth activists and first-time voters to resist and subvert government pedagogies and techniques of surveillance. This article reflects on the aspirations and strategies of young Malaysian citizens (with this study focusing on Malaysian-Chinese youth residing in Kuala Lumpur) who, in their interview responses, embodied a different kind of digital citizen subjectivity from the surveillant-citizen ideal expressed by stakeholders. More than anything, young people wanted to be free to engage in knowledge creation through social media and to express critical political and social views without fear of repercussion.

Although young people expressed hopes after GE14 that the result would give the new government a mandate to provide more opportunities for free expression and to enshrine these values in DC programs, while also abolishing the use of the Sedition Act for political purposes, this has not yet been realized, with the Sedition Act and the CMA continuing to be used to police online political expression. But this is not just a challenge for policymakers in Malaysia; rather, globally, the Control Paradigm that digital citizenship policy and programs are shown to embody, in this context and in others, continue to have unintended consequences which constrain young people’s agency and enjoyment of participation rights, making changes to policy settings an urgent priority.

References

Article 19. (2017). Malaysia: The Communications and Multimedia Act 1998: Legal Analysis, February 2017. Retrieved from https://www.article19.org/data/files/medialibrary/38689/Malaysia-analysis-Final-December.pdf

Andrejevic, M. (2005). The work of watching one another: Lateral surveillance, risk and governance. *Surveillance & Society*, *2*(4), 479–497.

Bahfen, N. (2009). Modems, Malaysia and modernity: Characteristics and policy challenges in Internet-led development. In G. Goggin & M. McLelland (Eds.), *Internationalizing Internet studies: Beyond anglophone paradigms* (pp. 163–178). New York, NY: Routledge.

Baym, N., & boyd, d. (2012). Socially mediated publicness: An introduction. *Journal of Broadcasting & Electronic Media*, *56*(3), 320–329. doi:10.1080/08838151.2012.705200

Bennett, W. L., & Segerberg, A. (2012). The logic of connective action. *Information, Communication & Society*, *15*(5), 739–768. doi:10.1080/1369118X.2012.670661

British Broadcasting Corporation. (2020, July 28). Najib Razak: Malaysian ex-PM gets 12-year jail term in 1MDB corruption trial. *BBC News.* Retrieved from https://www.bbc.com/news/world-asia-53563065

Cheong, N. (2021). Disinformation as a response to the ‘opposition playground’ in Malaysia. In A. Singpeng & R. Tapsell (Eds.), *From grassroots activism to disinformation: Social media in Southeast Asia* (pp. 63–85). Singapore: ISEAS Publishing.

Chinnasamy, S., & Azmi, N. M. (2018). Malaysian 14th general election: Young voters and rising political participation. *Journal of Social Sciences Research*, *4*, 125–138. doi:10.32861/jssr.spi4.125.138

Cho, A. (2019). Default publicness: Queer youth of color, social media, and being outed by the machine. *New Media & Society, 20*(9), 3183–3200. doi:10.1177/1461444817744784

Communications and Multimedia Act (Act 588). (1998). Retrieved from https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Act588bi_3.pdf

Haggerty, K. D., & Ericson, R. V. (2006). The new politics of surveillance and visibility. In K. D. Haggerty & R. V. Ericson (Eds.), *Surveillance and visibility* (pp. 3–35)*.* Toronto, ON: University of Toronto Press.

Harris, A. (2013). *Young people and everyday multiculturalism*. New York, NY: Routledge.

Harris, A., & Han, A. (2020). 1Malaysia? Young people and everyday multiculturalism in multiracialized Malaysia. *Ethnic & Racial Studies*, *43*(5), 816–834. doi:10.1080/01419870.2019.1580379

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2019). *Digital citizenship in a datafied society*. Cambridge, UK: Polity.

Isin, E., & Ruppert, E. (2015). *Being digital citizens*. London, UK: Rowman & Littlefield.

Jiow, H. J., & Morales, S. (2015). Lateral surveillance in Singapore. *Surveillance & Society*, *13*(3/4), 327–337. doi:10.24908/ss.v13i3/4.5320

Johns, A. (2020). "This will be the WhatsApp election": Crypto-publics and digital citizenship in Malaysia's GE14 election. *First Monday*, *25*(12). doi:10.5210/fm.v25i12.10381

Johns, A., & Cheong, N. (2019). Feeling the chill: Bersih 2.0, state censorship, and "networked affect" on Malaysian social media 2012–2018. *Social Media + Society*, *5*(2), 1–12. doi:10.1177/2056305118821801

Khoo, B. T. (2016). Networks in pursuit of a "two-coalition system" in Malaysia: Pakatan Rakyat's mobilisation of dissent between reformasi and the tsunami. *South East Asian Studies*, *5*(1), 73–91. doi:10.20495/seas.5.1_73

Koh, S. Y. (2017). *Race, education and citizenship: Mobile Malaysians, British colonial legacies, and a culture of migration*. New York, NY: Palgrave MacMillan.

Lim, M. (2016). Sweeping the unclean: Social media and the Bersih electoral reform movement in Malaysia. *Global Media Journal*, *14*(27), 1–20.

Lim, S. S., & Soriano, C. (2016). *Asian perspectives on digital culture: Emerging phenomena, enduring concepts*. New York, NY: Routledge.

Livingstone, S., & Bulger, M. (2014). A global research agenda for children's rights in the digital age. *Journal of Children and Media*, *8*(4), 317–335, doi:10.1080/17482798.2014.961496

Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New Media & Society*, *19*(5), 657–670. doi:10.1177/1461444816686318

Lyon, D. (2006). 9/11, synopticon, and scopophilia: Watching and being watched. In K. D. Haggerty & R. V. Ericson (Eds.), *Surveillance and visibility* (pp. 35–54). Toronto, ON: University of Toronto Press.

Malaysian Communications and Multimedia Commission. (2018). *User survey: Statistical brief 23*. Retrieved from https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Internet-Users-Survey-2018.pdf

Malaysian Communication and Multimedia Commission. (2020a). *Klik dengan bijak* [Click wisely]. Retrieved from https://klikdenganbijak.my/en/learn_more.php

Malaysian Communication and Multimedia Commission. (2020b). *Know the law*. Retrieved from https://klikdenganbijak.my/en/resources.php

Malaysian Communication and Multimedia Commission. (2020c). *Self-Regulation*. Retrieved from https://klikdenganbijak.my/en/resources.php

Marwick, A., & boyd, d. (2010). "I tweet honestly, I tweet passionately": Twitter users, context collapse, and the imagined audience. *New Media & Society*, *13*(1), 114–133. doi:10.1177/1461444810365313

McCosker, A. (2015). Managing cyberbullying: The three layers of control in digital citizenship. In A. McCosker, S. Vivienne, & A. Johns (Eds.), *Negotiating digital citizenship: Control, contest, culture* (pp. 21–39). London, UK: Rowman & Littlefield.

Mohd Hed, N., & Grasso, M. T. (2020). Age group differences in political activism in Malaysia. *Journal of Youth Studies*, *23*(6), 765–779. doi:10.1080/13676261.2019.1636948

Mohd Sani, M., Ahmad, M. Z., & Wahid, M. (2016). Freedom of the Internet in Malaysia. *The Social Sciences*, *11*(7), 1343–1349. doi:10.3923/sscience.2016.1343.1349

Mouffe, C. (2011). *On the political*. London, UK: Routledge.

Ong, A. (1999). *Flexible citizenship: The cultural logics of transnationality*. Durham, NC: Duke University Press.

Pink, S., Horst, H., Postill, J., Hjorth, L., Lewis, T., & Tacchi, J. (2016). *Digital ethnography: Principles and practice*. Los Angeles, CA: SAGE Publications.

Robards, B. (2013). Friending participants: Managing the researcher–participant relationship on social network sites. *Young: Nordic Journal of Youth Research*, *21*(3), 217–235. doi:10.1177/1103308813488815

Sedition Act. (1948). Retrieved from https://www.lawyerment.com/library/legislation/acts/1948/15/

Sergeant, G. (2018, May 12). Mahathir's back: Are we going to see a revival of the Asian Values debate? *Hong Kong Free Press*. Retrieved from https://hongkongfp.com/2018/05/12/lets-not-return-asian-values-debate-heads/

Sinpeng, A., & Tapsell, R. (2020). *From grassroots activism to disinformation: Social media in South-East Asia*. Singapore: ISEAS.

Tapsell, R. (2018). The smartphone as the "weapon of the weak": Assessing the role of communication technologies in Malaysia's regime change. *Journal of Current Southeast Asian Affairs*, *37*(3), 9–29. doi:10.1177/186810341803700302

Third, A., Bellerose, D., Dawkins, U., Keltie, E., & Pihl, K. (2014). *Children's rights in the digital age: A download from children around the world*. Retrieved from http://www.uws.edu.au/__data/assets/pdf_file/0003/753447/Childrens-rights-in-the-digital-age.pdf

Third, A., Collin, P., Walsh, L., & Black, R. (2019). *Young people in digital society: Control shift*. London, UK: Palgrave Macmillan.

Treré, E. (2015). Reclaiming, proclaiming, and maintaining collective identity in the #YoSoy132 movement in Mexico: An examination of digital frontstage and backstage activism through social media and instant messaging platforms. *Information, Communication & Society*, *18*(8), 901–915. doi:10.1080/1369118X.2015.1043744

UNESCO. (2015). Fostering digital citizenship through safe and responsible use of ICT: A review of current status in Asia and the Pacific as of December 2014. Retrieved from https://en.unesco.org/sites/default/files/sru-ict_mapping_report_2014.pdf

Weiss, M. L. (2013). Parsing the power of "new media" in Malaysia. *Journal of Contemporary Asia*, *43*(4), 591–612. doi:10.1080/00472336.2012.759332