John Postill, Victor Lasa und Ge Zhang

Monitory politics, digital surveillance and new protest movements: an analysis of Hong Kong's Umbrella Movement

Abstract: In this article we seek to inject some dynamism and complexity into the current scholarship on digital surveillance. Drawing from ethnographic research in Hong Kong, we argue that digital surveillance is a multi-directional endeavour with top-down, bottom-up and horizontal dimensions. Therefore it cannot be reduced to desktop-down portrayals of an almighty 'surveillance state' – not even in advanced surveillance regimes like China's. Instead we suggest that digital surveillance practices must be set within a much larger, dynamic system we describe as *monitory politics*, a type of political action in which state and non-state actors surveil and shape one another's activities across a rapidly changing communicative landscape. To develop this idea, we first provide a brief methodological section based on our participant observation during the 2014 protests in Hong Kong, also known as the Umbrella Movement, after which we review the existing literature on China's surveillance efforts. We then sketch an account of the protests, followed by a discussion of the uncannily similar horizontal (or lateral) surveillance practices of local people and the police. We conclude that China's 'networked authoritarianism' (MacKinnon 2011, 2012) is far from being a perfect model of control, for numerous forms of dissent and resistance survive in the country, with the Hong Kong protests as a case in point.

Introduction

The political theorist John Keane (2009) has argued that a new political form has spread around the world since 1945: 'monitory democracy'. This is the idea that decision-makers in all spheres of society – including government, the private sector and civil society – are subject to ever-increasing levels of public scrutiny. Monitory democracy does not replace representative democracy. Rather the two co-exist uneasily, with the irresolvable tension of mostly unelected actors guarding over elected representatives at its heart. Building on these ideas, and using Spain's *indignados* (15M) movement as their case study, Feenstra and Keane (2014) point out that today's monitory democracies must be understood in relation to a 'new architecture of communicative abundance'. In other words, we must take into account the explosive uptake of digital media we are currently experiencing (Feenstra and Keane 2014).

This suggests that we should understand digital surveillance policies and practices not in isolation, but in relation to much larger, changing sets of strategies and tac-

tics – some carefully crafted, others improvised as conditions change on the ground – deployed by governments, corporations and citizens.

Although there is a burgeoning literature on internet control by both autocratic and democratic states, to date there has not been much research on how governments are actually responding to the new protest movements beyond 'shutdowns' of the kind carried out by the Mubarak regime during the Egyptian uprising of 2011 (Tsui 2015). As Tufekci and Wilson (2012) and other authors have pointed out, governments around the globe have gradually come to realise that an internet shutdown is 'a crude or even desperate last resort' (Tsui 2015). Instead many governments are developing multi-pronged strategies. These include legal pushback tactics, flooding sites with hired 'trolls', targeted viruses, distributed denial-of-service (DDoS) attacks, increasing the cost of accessing 'undesirable information', takedown notices, stringent terms of usage policies, and surveillance at key points of the Internet's infrastructure (Deibert and Rohozinski 2010; Cayford, Pieters and Hijzen 2018; Tsui 2015).

To date China and Hong Kong have mostly resorted to censorship, demonisation of Western interference and digital surveillance in an effort to assert and consolidate their online authority (Feng and Guo 2012; Tsui 2015). Although until 2014 the Hong Kong government had 'little to no track record of online censorship' (Tsui 2015), loopholes in the existing legislation are allowing the authorities to conduct online surveillance with increasing ease. The Crimes Ordinance Section 161; for instance, originally intended as a tool against cyberfraud, is often deployed to quell online dissidence (Tsui 2015).

This picture would be incomplete, however, without accounting for the kinds of horizontal (or 'lateral', Andrejevic 2005) surveillance we consider below, including surveillance of citizens *by* citizens. In this article we seek to inject some dynamism and complexity into the current scholarship on digital surveillance. Drawing from ethnographic research in Hong Kong, we argue that digital surveillance is a multidirectional endeavour with top-down, bottom-up and horizontal dimensions. Therefore it cannot be reduced to desktop-down portrayals of an almighty 'surveillance state' – not even in advanced surveillance regimes like China's. Instead we suggest that digital surveillance practices must be set within a much larger, dynamic system we describe as *monitory politics*, a type of political action in which state and non-state actors surveil and shape one another's activities across a rapidly changing communicative landscape. To develop this idea, we first provide a brief methodological section based on our participant observation during the 2014 protests in Hong Kong, also known as the Umbrella Movement, after which we review the existing literature on China's surveillance efforts. We then sketch an account of the protests, followed by a discussion of the uncannily similar horizontal (or lateral) surveillance practices of local people and the police. We conclude that China's 'networked authoritarianism' (MacKinnon 2011; 2012) is far from being a perfect model of con-

trol, for numerous forms of dissent and resistance survive in that country, with the Hong Kong protests as a case in point.

Methodology

Our main research methods were ethnographic participant observation and informal interviews. During the first month of the protests, starting on 28 September 2014 when the police first fired teargas, one of the co-authors of this article was in Hong Kong. He visited a number of different protest sites on multiple occasions in the Central, Mong Kok, and Causeway Bay areas. Crisscrossing the camps at night he spoke to numerous protesters. There was a great deal of peaceful waiting and no shortage of time to kill, as well as much confusion about what was going on. He often sat at the protests sites and observed the crowds or browsed online on his smartphone. This allowed him to monitor the Facebook timeline and local Firechat chat groups sending and receiving messages about the latest protest developments. Sometimes in the middle of the night people would yell to warn other campers of a police charge so that they could begin to move away. Most of the time, however, it was fairly quiet and many interactions were mediated by applications like Firechat.

Our co-author spoke to university students, especially undergraduates who formed the bulk of the protest demographic. There were also high school students and some young office workers. The language spoken on protest sites was almost exclusively Cantonese, with English spoken only with the small numbers of primarily Western and South Asian residents that visited the sites. English was the preferred Facebook language, especially in daily conversation (partly because typing in English is faster). By contrast, on Firechat – an application that was only popular during the protests – Cantonese was more commonly used. Arguably this had to do with Cantonese being regarded as the more patriotic language.

The occupation sites were all but empty during the daytime hours, with some students on duty guarding them. They usually became busy after dinner as office workers and curious onlookers visited. Large numbers of people would spend the night there. Police raids were often conducted at night or in the early morning hours.

As observed in similar 'square protests' around the world (Postill 2014, 2018), the general mood among occupiers gradually shifted from an initial trepidation at the uncertain outcome of the protests to a growing tedium and fatigue, the only excitement being provided by petty squabbles or fights among participants. Eventually it dawned on occupiers that all that remained was for them to be cleared by the police.

The analysis below is based on a selection of materials gathered during this period, triangulated with scholarly and journalistic texts on digital surveillance and social protest in mainland China and Hong Kong. We focus on two main platforms:

Firechat and Facebook. Firechat was chosen for two reasons. First, because one of our key informants, who we shall call Cheung, had firsthand experience of it. Second, because of claims in the international media about its emancipatory potential during the protests. For its part, Facebook contributed to the considerable political confusion and horizontal surveillance practices that characterised the protests, including using it to expose and unfriend others for their actual or assumed stance on the unfolding conflict.

Internet and power in China

While in mainland China the government has taken a 'cautious and highly centralized' approach to the issue of Internet control, Hong Kong's approach has been more liberal in terms of censorship, technological development and universal access to Internet infrastructure (Yang 2007; Freedom House 2014; Tsui 2015). Hong Kong's Internet is one of the fastest in the world with a high penetration rate (73%) and up to 96% of mobile users accessing the Internet on a daily basis (Freedom House 2014; Go-Globe 2014). Online political dissent was traditionally exercised freely with no deterrents, and freedom of speech is protected by law (HKHRM 1991; Freedom House 2013). Until the current wave of political dissent ignited in 2011, the authorities acted with relative independence from mainland internet policies. Despite being identified by many observers as a growing problem, the mainland influence over Hong Kong authorities remains unclear. Still, analysing Chinese efforts to control the Internet is a useful exercise to understand the evolving policy framework in which Hong Kong authorities operate.

Jamison (2014) has investigated Chinese plans to establish 'national sovereignty' in cyberspace by taking over Hong Kong's internet. Certain information control actions by the Hong Kong authorities in recent years are showing an increasingly authoritarian tenor (Yang 2007; Freedom House 2013). In the words of China's President and Chinese Communist Party (CCP) General Secretary Xi Jinping in 2013; 'the Internet has become the main battlefield for public opinion struggle' (Freedom House 2014: 2). The Chinese-style of internet control can be described as a holistic approach to national information security. With the main goal of maintaining social control, this information security is understood as the elimination of risk in the creation, collection, processing and dissemination of publicly-available information by the citizens. The approach features three main categories of action: access control, content control and direct action against insurgent information-sharing and publishing (Feng and Guo 2012; Tsui 2015).

In mainland China, the most obvious manifestation of censorship is the difficulty in accessing foreign websites, a problem known as the 'Great Firewall of China' (MacKinnon 2011: 32). The analysis and study of this by Western observers created the 'Iron Curtain 2.0' discourse, which describes the Chinese regime as a strong censor obsessed with disconnecting its population from the openness of the Inter-

net. However, this Iron Curtain-style analogy has been strongly criticized in recent years by Asian academics like Lokman Tsui, who argue that it 'may indeed have blinded many Western policy makers, human-rights activists, and journalists to what is really happening in China' regarding not just internet policies but public opinion as well (Tsui in MacKinnon 2011: 36).

The way content control is exercised shows a sophisticated effort by Chinese authorities to create an illusion of freedom of speech while remaining in control of the major issues. MacKinnon (2011; 2012) describes this behaviour as 'networked authoritarianism', a situation in which a CCP-dominated political environment remains mainly in control while conversations about the country's problems are allowed on websites and social media. It follows that the average citizen 'with internet or mobile access has a much greater sense of freedom in ways that were not possible under classic authoritarianism, managing to have more fun, feel more free, and be less fearful of their government' than at the beginning of the 21st century (2011: 33). Online dissent will be allowed provided it is not about regime change, or 'exit strategies', including calls for an end of CCP rule.

Min Jiang describes this system as 'authoritarian deliberation'. This author explains how Chinese cyberspace has been divided by authorities into four main deliberative spaces: '1) *central propaganda spaces*, meaning websites and forums built and operated by the government; 2) *government-regulated commercial spaces*, that is, websites and digital platforms operated by private companies that are subject to government regulation; 3) *emergent civil spaces*, i.e. sites run by nongovernmental organizations and non-commercial individuals, which are censored less systematically than commercial spaces but are nonetheless subject to registration requirements such as intimidation, shut-down, or arrest when authors cross the line or administrators fail to control community conversations; and 4) *international deliberative spaces*, websites hosted overseas for content and conversations not allowed on domestic websites (Jiang in MacKinnon 2011: 36). This strategy is designed, supervised and applied by an agency called the State Internet Information Office. It was created in 2011 with the purpose of 'regulating online content, punishing violators, and overseeing telecommunications companies' (Freedom House 2014: 6).

While Jiang's 'international deliberative spaces' are subject to strong censorship by the 'Great Firewall of China', the other three environments are subject to a more subtle censorship, completed with associated propaganda and supervised via surveillance. Private corporations, including foreign ones, play a controversial role in contributing to censorship following government pressure in the 'government-regulated commercial spaces' (Freedom House 2014). For example, in August 2013 Weixin's international version WeChat suspended the account of an overseas web portal that is blocked in China. Keyword blacklists are regularly downloaded as updates to instant-messaging applications like Tom-Skype and QQ, while other companies 'employ people to delete posts', even before they reach the general public,

sometimes receiving 'as many as three censorship directives per day by text message, instant message, phone call, or e-mail' (2014: 10).

The result of such a holistic strategy is an approach to censorship and surveillance that facilitates supervision of political dissent at the grassroots level, including horizontal (or lateral) surveillance, as we will shortly explain. Consequently, in Hong Kong freedom of expression and the press were gradually eroded between 2007 and 2012 (HK Journalists Association 2012). Although there is no specific legislation in Hong Kong about press or internet control, government agencies issue regulation that allow to establish certain guidelines that translate into policies and specific actions (Freedom House 2014: 15; Tsui 2015).

As we can see, the extant academic and activist literature on internet control and surveillance in China and Hong Kong has to date focussed on official policy and legislation. As a result, we still know little about the authorities' strategy for on-the-ground, horizontal protest surveillance mediated by new apps and platforms, e.g. Firechat, or indeed about citizens' own forms of digital surveillance. After a brief overview of the 2014 protests, we will turn our attention to precisely this issue.

The Umbrella Movement

The 2014 Hong Kong protests, also known as the Umbrella Movement, began in late September 2014 as a civil disobedience campaign aimed at pressurising the Chinese government into implementing universal suffrage in the territory (Chow, Yau and Li 2015; Rodríguez 2014). This followed the Chinese government's scrapping of 'a fully democratic election for a new Hong Kong leader in 2017; as […] promised to them by Beijing in late 2007'. With this new decision, Beijing acquired total control over who could stand in that election (Ho 2015).

Khong (2015) regards these protests as a legacy of the 2011 uprisings around the globe, from the Arab Spring via Spain's *indignados* to the Occupy movement. In common with that earlier wave, 'social media took centre stage as a source for both information and mobilisation'. As the celebrated young activist Joshua Wong put it: 'Without Facebook there would be no Occupy Central, without Facebook there would be no Joshua Wong' (quoted in Khong 2015).

The protests started on 28 September, when students and other citizens demanding 'real democracy' pitched their tents on the streets of Hong Kong. Protesters occupied the city's main roads, set up encampments, organised supplies of food and water, and protected the occupied sites with barricades and human chains. As was the case in 2011 in countries such as Spain or the US (Postill 2014, 2018), the use of excessive force by the riot police, widely shared via social media, only helped to swell their numbers. Meanwhile both sides launched discreet cyber attacks through mobile phone applications using surveillance malware. They also sent phishing emails and launched distributed denial-of-service (DDoS) operations. At its peak,

over 100,000 people participated in the occupations until the police cleared the last remaining occupation site on 15 December 2014 (Chow, Yau and Lie 2015; Gillen 2015; Ho 2015; Yuen 2015).

Horizontal surveillance and social media

As explained earlier, one of the authors of the present article was a participant observer during the occupation phase of the movement. This section draws on his firsthand experience of the occupation sites as well as an extensive reading through Facebook timelines and Firechat logs. Contrary to Tsui (2015)'s view that the curtailing of online freedoms in Hong Kong is due solely to governmental surveillance and censorship, his online and offline experiences during the Umbrella movement enabled us to think about surveillance in more nuanced ways. This included paying attention to how protesters surveilled one another, or how the police had to interact with protesters on a level playing field when using certain digital platforms.

Below we view these dynamics through the lens of Andrejevic's (2005) notion of 'lateral surveillance', which we prefer to call *horizontal surveillance* for its closer metaphorical fit with the other two modalities, namely 'top-down' and 'bottom-up' surveillance. Andrejevic defines lateral surveillance as 'not the top-down monitoring of employees by employers, citizens by the state, but rather the peer-to-peer surveillance of spouse, friends, and relatives' (2005: 481). In other words, ordinary people are today equipped with 'technological capabilities previously held exclusive by corporate and state entities' and 'monitor other citizens' behaviour through nonreciprocal forms of watching' (Humphreys; 2011; p.577).

During the Hong Kong protests, all citizens were encouraged to participate in horizontal/lateral surveillance in the name of democracy. This entailed informing the collective (often via large group chat or public posts on social media) of suspicious individuals and activities, video-recording discordant and violent 'hired' thugs and police brutality, and revealing a friend's long concealed political position. We are far removed here, therefore, from recent debates around collective vs. 'connective' identity found in the social movements literature (e.g. Bennett and Segerberg 2012; Gerbaudo and Trere 2015), which tend to overlook the more unsavoury aspects of protest surveillance from all sides in a conflict.

Shortly into the protests many people in Hong Kong began to express their political position by tagging their Facebook profile pictures with a yellow ribbon (in support of the movement), a blue ribbon (against the movement) or a yellow and blue ribbon tied together (an ambiguous conciliating position). There was a notable absence of genuine political debate and reflection. Open discussion of politics was often avoided, with some regarding it as the work of 'leftist pricks' or 'communist spies'. Many discreetly unfriended Facebook friends for displaying a rival ribbon. One research participant reported losing ten friends during first few weeks of the

occupation alone. The viral video 'Today, I unfriended my mum'[1] was a good example of the political intensity and public performance of political positions.

Thus one of our key informants, the earlier mentioned Cheung, recalls an instance of public unfriending on Facebook of a police officer. The Hong Kong police had been a main target of public scrutiny and indignation following numerous cases of brutality and failed undercover work. As the accused police officer was not directly involved in the Occupy event, this case of public unfriending indicates that many participants were unreflexive in their 'political' positionings within interpersonal spaces, tarring all police officers with the same brush.

In the streets, protesters monitored suspicious instances of incivility, vandalism, and verbal abuse as possible signs of hired thugs or undercover police attempting to shatter the peaceful and ordered nature of the protest so as to justify further crackdowns. In a sense, at the occupation sites there was a surveillance contest between protesters and undercover police. The contest cannot be easily explained away as a neat contrast between the top-down surveillance of the police and bottom-up surveillance of the protesters, as Pan (2010) summarised it in her study of Chinese crowdsourced surveillance. In fact, the surveillance practices of the police and protesters were uncannily similar. The similarity was the result of both sides seeking to show the other side in a poor light (for a Spanish parallel, see Postill 2015). This played out in three main contexts, namely in the streets, on camera and on Firechat. Thus police reportedly hired 'thugs' or went undercover to observe and disrupt the crowds. In turn, protesters found creative ways to provoke the police so as to elicit violent responses. Whilst police used video cameras to record the faces of protesters, these used their smartphones to record any 'uncivil' behaviour from the riot police. Moreover, leading protesters used Firechat to organise actions, make announcements and share information, while less involved participants used it to stay abreast of the latest developments. The police allegedly monitored this information and hired online trolls to create animosity and disharmony among the demonstrators. For this reason protesters warning people not to engage in 'pointless' debates mushroomed at protest sites.

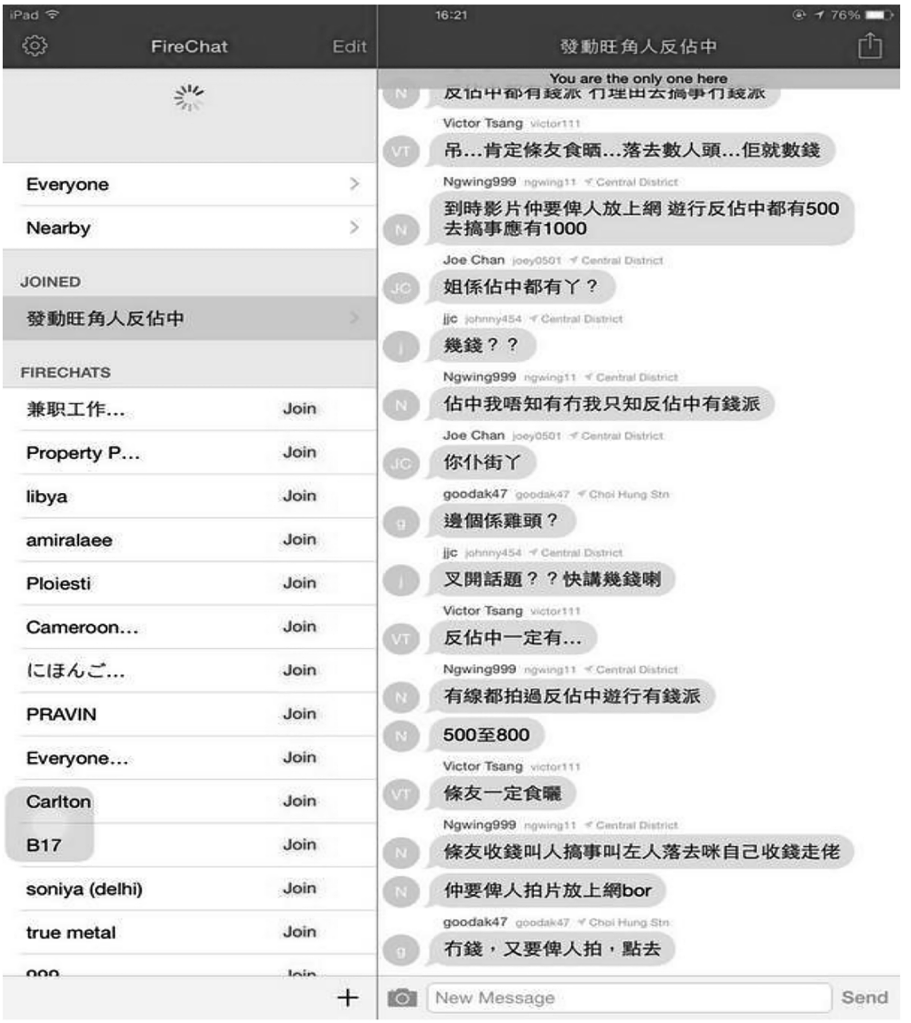
The public vigilance of surveillance (in particular, on the police and suspected hired thugs) through mobile devices was envisaged as visual evidence of prospective false accusations against peaceful protesters. Eye/camera-witness accounts were viewed as proof of the 'contrived character' of police testimonials – 'a mistrust of what is said in favour of what can be detected' (Andrejevic 2005: 482).

Most protesters were well aware of the authorities' monitoring strategies and correspondingly adopted alternative technologies that were thought to be secure. Thus Firechat, which is a location-based chatroom application that runs on Bluetooth

1 http://www.visiontimes.com/2014/11/12/how-the-umbrella-revolution-is-dividing-families-in-hong-kong-video.html (a report on this video).

rather than requiring a mobile internet connection, was a preemptive move aimed at overcoming the anticipated internet shutdown. It was creatively appropriated for the pragmatic use of organising protesters and goods. It soon became a fourth occupation site, as well as opening a new space for dissonant information.

Figure 1: Screenshot of public chatroom entitled 'Mobilise Mongkok against the Occupy-central'[2]



2 Translation of the conversation: 'protest against occupycentral you get 500, if you go stir up shit you can probably get 1000', 'I get money even from joining occupycentral?', 'How much?', 'I am not sure about occupying central I am sure you can earn money if you are on the side of antioccupy', 'fuck you', 'who is chicken head [cantonese slang for pimp]?', 'don't divert

On Firechat, there were many different channels for different purposes. Some were explicitly for information, e.g. for distribution of goods and location-based live news of police whereabouts; others were topic-based discussions and even advocacy groups temporarily migrated to them from online discussion boards. The above screenshot shows how anonymous participants discussed and spread information about financial rewards during the protest. It offers us a tantalising glimpse into the diversity of groups operating on Firechat and their different motivations for using this platform.

Horizontal (or lateral) surveillance as a concept is not necessarily adequate to understanding the novelty of Firechat but it is useful as an analytical entry point. Firechat's infrastructural features prevent top-down surveillance. Instead, the platform provides a level playing field for mutual, horizontal surveillance. The relative anonymity and collectivism of Firechat means it is unsuited to the task of tracking down individuals yet it is an ideal platform to monitor and spread brief items of (mis)information. It is particularly useful with slow or non-existent mobile internet connections. Anyone, including police officers and governments, can join the chat and post information. Influence is gained and lost through words and arguments that include rumours, lies and misinformation. Put differently, this is no Habermasian public sphere where critical-rational discourse can flourish.

In the Hong Kong context, there is a certain tech-savvy reputation associated with instant messaging applications such as Firechat or Telegram, which are often assumed to be superior to more popular apps such as Whatsapp and Facebook Messenger. This is partly due to how these platforms promote themselves as messaging applications that provide options for peer-to-peer exchanges instead of relying entirely on centralised servers. In everyday understandings, surveillance implies both asymmetry and non-transparency, whilst interactive technologies such as Firechat are marketed to be the exact opposite: as anti-surveillance tools. Such narrative fosters the optimistic view that such apps promoting participatory democracy. Despite being initially celebrated in Hong Kong as an instrument of democracy, Firechat was soon declared to be unsafe by both the mainstream and independent media. It was in this context that the participatory promise of social media began to be widely questioned – rather than taken for granted – in Hong Kong.

Conclusion

In the age of ubiquitous mobile and online media, surveillance is by no means the exclusive preserve of states and corporations but rather a multi-directional, multi-level phenomenon. This is not merely a matter of governments surveilling citizens or corporations surveilling customers, ordinary citizens in turn surveil governments

the topic, tell me how much is it', 'I am sure there is money if you are against occupy', 'even the cable tv has shot that antioccupy has money to offer', '500 to 800'…
.

and corporations – as well as one another. The Hong Kong protests show that even China's sophisticated 'networked authoritarianism' (MacKinnon 2011; 2013) approach to what we have termed monitory politics is far from watertight, as it allows for a range of forms of (digital) dissent to live on.

The media activist and researcher Ethan Zuckerman (2014) borrows the notion of 'monitorial citizenship' from Schudson to refer to citizens' responsibility 'to monitor what powerful institutions do (governments, corporations, universities and other large organizations) and demand change when they misbehave. The press is a powerful actor in monitorial democracies […]. And new media may broaden the potential for monitorial democracy, allowing vastly more citizens to watch, document and share their reports'. Commendable as this normative goal is, our research shows that monitorial citizenship in Hong Kong is a complex, morally contradictory form of political engagement, with expressions of selfless devotion to the lofty cause of democracy living alongside 'uncivil' forms of peer-to-peer surveillance via seemingly benign platforms such as Firechat. The result of our analysis is a dynamic, multidimensional picture of digital surveillance in Hong Kong, and probably elsewhere. The extant scholarship tends to produce rather static portrayals of 'cyber-policing' as a desktop-based, remote mass practice but misses out on more agile, on-the-ground policing practices – including the quasi- and counter-policing practices of protesters and other citizens.

References

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

Bennett, W. L. / Segerberg, A. (2012): The logic of connective action: Digital media and the personalization of contentious politics, in: *Information, Communication & Society 15*(5), 739-768.

Cayford, M., Pieters, W., & Hijzen, C. (2018). Plots, murders, and money: oversight bodies evaluating the effectiveness of surveillance technology. *Intelligence and national security*, 33(7), 999-1021.

Chan, J. (2008): The new lateral surveillance and a culture of suspicion, in: *Sociology of Crime Law and Deviance 10*, 223–239.

Chow, K. P., Yau, K. / Li, F. (2015): Cyber Attacks and Political Events: The Case of the Occupy Central Campaign, In: *Critical Infrastructure Protection IX,* pp. 17-27.

Deibert, R. / Rohozinski, R. (2010): Cyber wars, in: *Index on Censorship 29*(1), 79-90.

Feenstra, R. A. / Keane, J. (2014): Politics in Spain: A case of monitory democracy. *VOLUNTAS: International Journal of Voluntary and Nonprofit Organizations*, Online First, 1–19. doi:10.1007/s11266-014-9461-2

Feng, GC and Guo, SZ (2013), 'Tracing the route of China's Internet censorship: An empirical study', in: *Telematics and Informatics* 30, 335-345.

Freedom House (2013), 'Freedom of the press report', Freedom House, viewed on 15 May 2015, https://freedomhouse.org/report/freedom-press/2013/hong-kong

Freedom House (2014), 'Freedom on the net report: China', Freedom House, viewed on 15 June 2015, https://freedomhouse.org/report/freedom-net/2014/china

Fu, K. W. / Chan, C. H. (2015): Networked collective action in the 2014 Hong Kong Occupy Movement: analysing a Facebook sharing network. In *International Conference on Public Policy, ICPP 2015*.

Fuchs, C. (2012): Political Economy and Surveillance Theory, in: *Critical Sociology*, 39 (5), 671-687.

Rodríguez, S. M. (2014): Has social media fundamentally altered the role of the media in conflict, or simply speeded up the normal process of communication? November 2014, University of Kent, https://bit.ly/2woIbS6.

Gerbaudo, P. / Treré, E. (2015): In search of the 'we'of social media activism: introduction to the special issue on social media and protest identities, in: *Information, Communication & Society* 18(8), 865-871.

Gillen, J. (2015): Yellow umbrellas–recontextualisation in multimodal literacy practices of the Hong Kong student protests of November 2014. Discussion paper, Lancaster University, http://eprints.lancs.ac.uk/73260/

Go-Globe (2014), 'Internet usage in Hong Kong: statistics and trends', Go-Globe, viewed on 15 May 2015, http://www.go-globe.hk/blog/internet-usage-hong-kong/

Guittet, E.P. (2015): How generalised suspicion destroys society. *Open Democracy*. Access at https://www.opendemocracy.net/can-europe-make-it/emmanuelpierre-guittet/how-generalised-suspicion-destroys-society

HKHRM (1991), 'Hong Kong Bill of Rights', Hong Kong Human Rights Monitor, viewed 15 may 2015, http://www.hkhrm.org.hk/english/law/eng_boro1.html

HK Journalists Association (2012), 'Survey: Government manipulation eroded press freedom', Hong Kong Journalists Association, viewed 15 May 2015, http://www.hkja.org.hk/site/portal/Site.aspx?id=A1-1003&lang=en-US

Ho, K. (2015): Occupy Central: The Framing Contest of the Umbrella Movement in Hong Kong. Bachelor Thesis, University of Leiden, https://openaccess.leidenuniv.nl/handle/1887/33570

Humphreys, L. (2011): Who's watching whom? A study of interactive technology and surveillance, in: *Journal of Communication 61*(4), pp.575–595.

Jamison, J (2014), 'China's Internet agenda', The Diplomat, viewed on 15 May 2015, http://thediplomat.com/2014/12/chinas-internet-agenda/

Keane, J. (2009): *The life and death of democracy*, London.

Khong, E.L. (2015) Hong Kong's new struggle: the battle for digital rights, *Prospect Magazine*, 1 September http://www.prospectmagazine.co.uk/world/hong-kongs-new-struggle-the-battle-for-digital-rights

Loo, BPY (2004), 'Telecommunications reforms in China: towards an analytical framework', in: *Telecommunications Policy* 28, 697–714.

Lyon, D. (2014): Surveillance, Snowden, and Big Data: capacities, consequences, critique, in: *Big Data & Society* 1(2), 1–13.

MacKinnon, R (2011), 'China's networked authoritarianism', in: *Journal of Democracy* 22(2), pp.32-46.

MacKinnon, R. (2012), *Consent of the Networked*, New York.

Mahrt, M. / Scharkow, M. (2013): The value of Big Data in digital media research, in: *Journal of Broadcasting & Electronic Media 57*(1), pp.20-33.

Mann, S., Nolan, J. / Wellman, B. (2003): Sousveillance : Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments, in: *Surveillance and Society 1*(3), pp.331–355.

Pan, X. (2010): Hunt by the crowd: An exploratory qualitative analysis on cyber surveillance in China. *Global Media Journal 9*(16), 1-19.

Pieterse, JN (2012): 'Leaking Superpower: WikiLeaks and the contradictions of Democracy', in: *Third World Quarterly*, 33(10), 1909-1924.

Pink, S., H. Horst, J. Postill, L. Hjorth, T. Lewis and J. Tacchi (2016): *Digital Ethnography: Principles and Practice.* London.

Postill, J. (2008): Localizing the internet beyond communities and networks, in: *New Media & Society* 10(3), pp.413-431.

Postill, J. (2012) Digital politics and political engagement, in: Horst H, Miller D (eds*), Digital Anthropology,* Oxford.

Postill, J. (2014) Spain's indignados and the mediated aesthetics of nonviolence, in P. Werbner, K. Spellman-Poots and M. Webb (eds), *The Political Aesthetics of Global Protest: Beyond the Arab Spring*. Edinburgh, pp. 341-367.

Postill, J. (2018): *The Rise of Nerd Politics*. London: Pluto.

Postill, J. & Pink, S. (2012): Social media ethnography: The digital researcher in a messy web, in: *Media International Australia* 145, 123–134.

Snijders, C., Matzat, U. / Reips, U. D. (2012): Big Data: Big gaps of knowledge in the field of internet science, in: *International Journal of Internet Science 7*(1), pp.1-5.

Stockmann, D. (2015): Big Data from China and its Implication for the Study of the Chinese State--A Research Report on the 2014 Hongkong Protests on Weibo. *Available at SSRN 2607998*.

Trottier, D. (2011): Mutual Transparency or Mundane Transgressions? Institutional Creeping on Facebook, in: *Surveillance & Society 9*(1-2), pp.17–30.

Trottier, D. (2012): Interpersonal Surveillance on Social Media, in: *Canadian Journal of Communication 37*(2), pp.319–332.

Tsui, L (2015), 'The coming colonization of Hong Kong cyberspace: government responses to the use of new technologies by the umbrella movement', in: *Chinese Journal of Communication*, DOI: 10.1080/17544750.2015.1058834

Tufekci, Z. and C. Wilson (2012): Social media and the decision to participate in political protest in Egypt: Observations from Tahrir Square, in: *Journal of Communication* 62(2): p.365.

Qiang, X (2011), 'The battle for the Chinese internet', *Journal of Democracy*, Volume 22, Number 2, April 2011, pp. 47-61.

Yang, KCC (2007): 'A comparative study of Internet regulatory policies in the Greater China Region: Emerging regulatory models and issues in China, Hong-Kong SAR and Taiwan', *Telematics and Informatics*, 24 (2007), 30-40

Yuen, S. (2015): Hong Kong after the Umbrella Movement: An Uncertain Future for One Country Two Systems, in: *China Perspectives* (1), p.49.

Zuckerman, E (2014): Promise tracker and monitorial citizenship, *My Heart's in Accra*, 24 January, http://www.ethanzuckerman.com/blog/2014/01/24/promise-tracker-and-monitorial-citizenship/#sthash.xy5g8AVX.dpuf

Dr. John Postill
Digital Ethnography Research Centre
RMIT University
VIC 3000 Melbourne
Australia
john.postill@rmit.edu.au

Victor Lasa
School of Global, Urban and Social Studies
RMIT University
VIC 3000 Melbourne
Australia
s3375621@student.rmit.edu.au

Ge Zhang
Digital Ethnography Research Centre
RMIT University
AU-VIC 3000 Melbourne
Australia
playbourer@gmail.com