Journal of Contemporary Governance and Public Policy, 3 (1) April 2022, 31-46
ISSN: 2722-3981 (Print), ISSN: 2722-3973 (Online)
Available Online at https://journal.ppishk.org/index.php/jcgpp

JOURNAL OF CONTEMPORARY GOVERNANCE AND PUBLIC POLICY

Terrorism Industry and Data Coloniality in Southeast Asia

Mohammed Ilyas[1]*

[1] Department of Sociology, Social Policy and Criminology, University of Liverpool, United Kingdom

*Corresponding Author Email: m.ilyas@liverpool.ac.uk

Received: 28 Oktober 2021; Revised: 10 March 2022; Accepted: 22 March 2022

Abstract

Decolonisation of academia has become a 'vogue' among scholars, students and activists, which has resulted in many publications on decolonisation. Unlike the social sciences, the online world and digital data have not received much attention from decolonial scholars. Digital data colonialism combines historical colonialism's predatory aspect and computer science ability to quantify and commodify online relations. The organisations responsible for digital data colonialism are big tech companies and powerful Western countries' intelligence agencies. Tech companies gather digital data and sell it for profit to big businesses. While, intelligence agencies of powerful Western gather digital data and use it for national interest and securitisation of populations under the banner of fighting terrorism, which reproduces non-Western countries' coloniality. This paper discusses the coloniality of non-Western countries by powerful Western countries through the use of digital data colonialism, which is carried out by their inelegance agencies and Western tech companies.

Keywords: *Data Colonialism; Coloniality; Securitisation; Intelligence Gathering*

Copyright © 2022 by Author, Published by Pusat Penelitian Ilmu Sosial dan Humaniora Kontemporer, Indonesia. This is an open access article under the CC BY-SA License (https://creativecommons.org/licenses/by-sa/4.0).

How to Cite: Ilyas, M. (2022). Terrorism Industry and Data Coloniality in Southeast Asia. *Journal of Contemporary Governance and Public Policy, 3*(1), 31-46. https://doi.org/10.46507/jcgpp.v3i1.65

Permalink/DOI: https://doi.org/10.46507/jcgpp.v3i1.65

Introduction

Over the last few decades discussing colonialism, decolonisation and coloniality have gained much traction among scholars and students in Western and non-Western countries (Said 1979; Connell 2007; Alatas 2000; Grosfoguel 2013; Mignolo 2011; Mwambari 2020; Kwet 2019; Steinmetz 2017). These discussions have led to two things. Firstly, calls to decolonise the social science and humanities subjects, but this is only in a few countries such as South Africa, UK and the US (Bhambra et al. 2018). Secondly, scholars such as Tuck and Yang (2012) have called for decolonisation to be more radical and engage in 'practical decolonisation' and avoid 'moves to innocence. However, until recently, there has been little discussion on digital data colonialism by Western tech companies and powerful Western countries' intelligence agencies. Scholars have discussed ownership, access to the Internet, Internet infrastructure and how Western tech companies such as Facebook, Google, Apple and Amazon use customer data (Zuboff 2019; Mejias and Couldry 2020; Jim et al. 2016; Kwet 2019; Coleman 2019; Pinto 2018; Youn 2019; Monique and Angela, 2019; Notias 2020). The Snowden leaks in 2013 led to some discussion about data gathering by the intelligence agencies of powerful Western countries and allied countries (Five Eyes, SIGINT Senior Europe and SIGINT Senior Pacific), but these discussions were not framed through a decolonial lens. Digital data gathered by intelligence agencies from the Internet, surveillance cameras, tracking devices, biometric machines, satellites, geospatial mapping technology and drones affords powerful Western countries their allies a lot of power to securitise populations and maintain economic and political dominance over rival countries (The Intercept 2018; Dorling 2014; UNHCR 2015; Thoma 2018, Kaurin, 2019; Jacobson 2017; Mejias and Couldry 2020; Babuta et al. 2020). The power comes from the knowledge produced from the digital data, which is used to develop securitisation policies.

This situation has also led to what Byler and Boe (2019) call 'terror capitalism', which has its roots in the 'War on Terror'. The war justified the development and use of digital data gathering surveillance technology in counter-terrorism programs in many countries, at the expense of human rights. One example of this is an Israeli company called Faception is offering technology to detect terrorists, and in Berlin, such technology has already been tried out (Faception 2020; Baz 2019; Huggler 2017). Another example is NSO, an Israeli company that develops sophisticated spyware, which is sold to many governments and security agencies to spy on people deemed a 'threat' to the state's national interest (Marczak et al. 2018). Chinese companies such as Yitu worked with the Malaysian government to develop artificial intelligence (AI) software (facial recognition) to help Malaysian police identify criminals (Tao 2018). Using digital data to develop the technology mentioned above raises several serious ethical issues, such as extrajudicial killings because of racist algorithms and AI being racist. An excellent example of this is the 'Future Dangerousness' program used by US courts (O' Neil 2016). Although digital data colonialism affords powerful Western countries a lot of economic and political power, this is not without criticism from Western civil rights groups, who have asked serious questions about data privacy and the digital data's final use (Mejias and Couldry

2020). Even though civil rights groups raise ethical concerns, these concerns seem to be limited to what happens in Western countries. There is little focus on the impact that digital data colonialism is having in non-Western countries.

This paper employs the definition of the terrorism industry, as developed by Herman and O' Sullivan (1989: 55-213). The terrorism industry is composed of the intelligence agencies of powerful Western countries and their allies, think tanks, lobbying organisations, research centres, security firms, scholars, media firms, private military firms, tech companies and NGOs. All of them are located in powerful Western countries or allied countries. The terrorism industry is an offshoot of counterinsurgency studies and emerged in the 1970s to counter the threat posed by the Soviet Union, and over the last few decades, has produced an abundance of knowledge about terrorism and related issues (Stampnitzky 2014). During colonial times, in countries like Malaysia, counterinsurgency played a pivotal role in undermining the Malaysian independence movement (French 2011; Hack 1999, 2009). Any counterinsurgency's success is based on data gathered on a movement or group that is considered to pose a risk to any given country's interests or occupying force (Komer 1972; Yazid 2019; Comber 2008; Karari 2018; Balce 2016). As a successor to counterinsurgency studies, the intelligence gathering side of the terrorism industry continues to gather data on populations, movements and groups that, for example, countries like the US and the UK deem as posing a risk to their national interests by using technology, which is far more sophisticated than their predecessors used.

This paper has a modest remit and aims to start a discussion on the relationship between the terrorism industry and digital data colonialism and the continuity of coloniality of non-Western countries. The paper focuses on the intelligence agencies of powerful Western countries and their allies (Five Eyes, SIGINT partners and SIGINT Pacific) because they are part of the terrorism industry and play a vital role in coloniality non-Western countries. The intelligence-gathering agencies provide the data and knowledge to develop strategies and programs that enable non-Western countries to reproduce coloniality. The paper has three sections. The first section introduces decolonial concepts that inform the paper. The second section discusses how powerful countries' intelligence agencies and Western tech companies work together to ensure that non-Western countries' coloniality continues. The paper concludes by urging fellow scholars to do two things. Firstly, adopt the decolonial approach and analyse how the industry engages in digital data colonialism and reinforces coloniality. Secondly, scholars concerned about the decolonisation of non-Western countries need to develop ways to implement Tuck and Yang's (2012) advice on undoing non-Western countries' coloniality.

Decolonial Concepts

The first decolonial concept that is relevant for this paper is digital data colonialism. Digital data colonialism is something that tech companies like Facebook and Google do, and it involves predatory colonialism, data extraction, data quantification and data

commodification of digital data (Couldry and Mejias 2019; Doffman 2019). Digital data colonialism is also a part of what Zuboff (2019) calls surveillance capitalism, which is the economic order that deems 'human experience' as free raw material, which is extracted from interactions between humans and technology and used for profit and developing technology that is used for predicting human behaviour. Predictive behaviour modelling generates profit for big business (Kachamas et al. 2019) and provides governments, such as the UK government, a way to predict radicalisation and terrorism (McKendrick 2019). That said, digital data colonialism and surveillance capitalism are impossible to escape because societies rely on and need more artificial intelligence technology to make 'life easier' such as Google Home, home robots and very soon driverless cars. This situation means that people have become trapped in a cycle of being 'sources of extraction, prediction, and consumption'.

However, digital data colonialism is not only carried out by Western tech companies, but as mentioned earlier, powerful Western countries and their allies also engage in digital data colonialism. The current definition of digital data colonialism is somewhat restrictive and needs expanding to include the intelligence-gathering practices carried out by the intelligence agencies of powerful Western countries and their allies. These practices involve intelligence gathering by a 'network of intelligence agencies belonging to powerful Western countries and their allies that use sophisticated surveillance and data extracting technology. The network is led by the US and the UK and assisted by allied countries. The motivation behind digital data colonialism for powerful Western countries is not profit, but profit can be one outcome. The main reason is to gain an economic and political advantage over rivals, which means securitisation of resource-rich non-Western countries and populations deemed dangerous. The world was made aware of digital data colonialism by powerful Western countries' intelligence agencies when Edward Snowden leaked NSA secret documents that detailed how the US and UK gathered social media users' data and spied on friendly and non-friendly governments. The leaks revealed the sheer amount and scope of digital data colonialism carried out by the countries mentioned and not surprisingly received much criticism from civil rights groups and the European parliament.

One way to understand the power that digital data colonialism affords powerful Western countries and their allies is to think about it at one level as providing a 'God-Eye view' (seeing and knowing everything) and at another level having an omnipresence of being everywhere at all times by using surveillance technology. The God-Eye view mentioned above is a continuation of the God-Eye view that resulted from the 16th-century genocides and epistemicides, which created the conditions for Descarte's to come up with his famous phrase, 'I think, therefore I am' (Grosfoguel 2013). The 'I' in the phrase refers to the white Western man and his culture and his modes of knowledge as superior, as well as to a quality of 'being' that enables him to think, produce knowledge, and have agency (Grosfoguel 2013). The opposite of the phrase, as Maldonado-Torres (2014) mentions, 'I do not think, therefore I am not', which means that everyone who is not Western and a white male is not only inferior, but his or her culture and modes of knowledge are also inferior. He or she is neither credited with the qualities of the white

man (Quijano 2007). Today, Descarte's 'I' can refer to powerful Western countries and their allies because digital data colonisation affords them great power and control to colonise the present and future and therefore create, direct, manage and control the future of non-Western countries.

The second concept is coloniality, which Mignolo (2011) calls the dark side of modernity. For Mignolo (2011), modernity and coloniality are interconnected and inseparable. This power arrangement has come to define all aspects of life, including culture, education, politics and knowledge production (Maldonado-Torres 2007; Grosfoguel 2006). Coloniality has three parts. Firstly, the coloniality of power, secondly, the coloniality of knowledge and finally, the coloniality of being. All three explain different aspects of coloniality (Ndlovu-Gatsheni 2013). The coloniality of power is the continuation of colonial structures of domination based on race and racism, which intersect with other categories and are the organising principle that structures other hierarchies of capitalism, such as labour and gender (Grosfoguel 2011). At the institutional level, coloniality of power is visible in how international financial and political organisations like the IMF, the World Bank, NATO, EU and the UN operate (Ndlovu-Gatsheni 2013; Grosfoguel 2006). The coloniality of knowledge refers to how local knowledge, modes of imagining and knowing the world have been replaced by Eurocentric knowledge because of its claim to scientific-ness. This situation results from the epistemicide of non-Western knowledge and religions (Ndlovu-Gatsheni 2013; Grosfoguel 2006; Quijano, 2007). Typically, coloniality of knowledge creates intellectual imperialism and a 'need' among some non-Western scholars to seek validation from Western scholars because of Western epistemology's dominance over non-Western epistemologies and its claim to universalism and objectivity (Bolivar 2010; Alatas 2000; Santander 2010; Grosfoguel 2006; Santos 2014, 2018). However, coloniality of knowledge in the context of digital data gathered by tech companies on behalf of powerful Western countries and Western countries' intelligence agencies maintains coloniality of non-Western countries by using digital data to fulfil economic, political and security policy goals.

The third part of coloniality is the coloniality of 'being', where the West is the zone of being and the non-West the zone of non-being. This binary is premised on Descarte's famous quote 'I think therefore I am', which means that only Western white men can think and therefore have the quality of existence and the 'Other' does not (Maldonado-Torres 2007; Grosfoguel 2016). The zone of non-being is the culmination of the coloniality of power and knowledge and operationalised to dehumanise and carry out violence on those below the abyssal line. An excellent example of this is the 'War on Terror', and how it created another line abyssal between Muslims and non-Muslims. Muslims occupied resided below the line of abyssal, which meant the surveillance of Muslims, data gathering on the religiosity and politics of Muslims, and violence inflicted on Muslims in form drone strikes, extrajudicial killings and torture (Raphael et al. 2016; Gordon, 2016; Gallagher, 2015; Fisher, 2013).

Intelligence Agencies and Coloniality

As mentioned earlier, the terrorism industry is comprised of many actors, including the intelligence agencies of powerful Western countries and tech companies. This section will discuss how these intelligence agencies and, in some cases, with Western tech companies' help maintain the coloniality of non-Western countries.

Until the Snowden leaks, the world knew very little about the digital data colonialism carried out by powerful Western countries' intelligence agencies. The Snowden leaks mentioned that the intelligence agencies of the US (National Security Agency - NSA) and the UK (Government Communications Headquarters - GCHQ), with the assistance of allied countries and Western tech companies, tapped into Submarine cables and colonised the Internet data produced by Internet users from many countries, including from their own (MacAskill et al. 2013; Davenport 2015; Ball 2013).

The Snowden leaks made the world aware of global intelligence-gathering networks composed of intelligence agencies of powerful Western countries and their allies, dating back to the Second World War. There are many networks, but the most important and powerful one is called the Five Eyes, which is the successor to the signals intelligence cooperation (SIGINT), which was set up during the Second World War by the US, UK and Australia (O'Neil 2017). After the war, the Five Eyes network was set up by the US and UK and included three other English-speaking countries: Canada, Australia and New Zealand (O'Neil 2017). Apart from the UK, the other countries are former colonies of the UK and settler states. These countries have mutual interests in joining the network and bringing capabilities that the others do not have, such as technology and geographical location. From the outset, the network heavily relied on technology. When satellite technology was developed, the network used it to develop a sophisticated digital data colonising program called Echelon that enabled the network to monitor all types of private and public sector organisations in all most every country (O'Neil 2017). The Five Eyes network colonised digital data from many countries, not only for security reasons but also to gain an economic and political advantage. The United States is responsible for SIGINT in Latin America, most of Asia, Russia, and northern China. At the same time, Australia is responsible for its neighbours (such as Indonesia), China, and Indo-China nations. Britain is responsible for Africa and the former Soviet Union, West of the Urals. Russia's polar regions are Canada's responsibility, and New Zealand's area of responsibility is the Western Pacific. (Richelson, 2012).

The remit for intelligence gathering of the Five Eyes members is quite extensive. It seems as though the goal of the network is to know everything about every other country. Be this be on security, politics or economics. In 1982, the US set up another network called SIGINT Seniors Europe, and it primarily focussed on the Soviet Union because of the Cold War. The initial and core members of SIGINT Seniors Europe are the Five Eyes members. Around the same time, the terrorism industry also started to produce much literature on the Soviet Threat (Stampnitzky 2014).

However, it was not until 9/11 that the Five Eyes and SIGINT Seniors Europe started to focus on counter-terrorism (Solon 2017; The Intercept 2018). As of 2013, the Five Eyes

mutated into what is called Fourteen Eyes, with the following countries: Belgium, Denmark, France, Germany, Italy, the Netherlands, Norway, Spain, and Sweden (Gallagher 2018). Sometimes the Fourteen Eyes is also called The SIGINT Seniors Europe and vice versa, which is somewhat confusing because both networks consist of the same countries (Gallagher, 2018). Aside from setting up the Fourteen Eyes and SIGINT Seniors Europe, the US also set up the SIGINT Pacific division in 2005, called SIGINT Seniors Pacific. The Pacific division is composed of the Five Eyes members and South Korea, Singapore, Thailand, France and India, and its goal is to monitor the Asia/Pacific regions and fight terrorism (Snowden 2007; Gallagher 2018).

The SIGINT network is extensive and involves many Western and non-Western countries, with some of them leading the network, such as the US and UK, while others act as data providers. The most crucial relationship in the SIGINT networks is between the US and the Second Parties, who are members of the Five Eyes, especially the UK (Greenwald 2014). The relationship between the US and other Third Parties is less critical, but the US has bilateral security agreements with some of them. Despite not being as important as the Second Parties members, the Third Parties members play a pivotal role in providing intelligence to the US and other Five Eyes members, vital to the continued coloniality of non-Western countries. Apart from the Five Eyes, the US also has strong relationships with members of SSPAC (SIGINT Seniors Pacific), SSEUR (SIGINT Senior Europe) and NATO (North Atlantic Treaty Organization) and Israel (Greenwald 2014; Giosue 2019).

Having all SIGINT partners in one extensive network means that the US and the other Five Eyes members have more eyes and more ways to colonise digital data from more countries. This situation vastly improves the capabilities of the Five Eyes members and the network. For example, France's inclusion means that digital data from parts of Africa, South America, and Russia can be gathered more efficiently because of France's capabilities (Pfluke 2019). Including South Korea and Germany in the network allows the network to keep a closer eye on North Korea (Pfluke 2019).

Until the Snowden leaks, little was known about how the intelligence agencies of powerful Western countries engaged in digital data colonialism. Key members of the networks tapped into Submarine cables to gain access to the Internet and other communication data and use spying technology to ears drop on world leaders, including leaders of countries that are members of the networks, such as Chancellor Merkel of Germany. The NSA called its digital data colonising programme PRISM, and GCHQ called its programme Tempora (MacAskill et al. 2013; Greenwald and MacAskill 2013). These programs specifically targeted the Internet data by tapping into Submarine cables that are the backbone of the Internet and other communication types (Digital Methods Initiative, 2020). The tapping enabled the intelligence agencies to colonise a tremendous amount of Internet data from Internet users from Western and non-Western Internet.

The submarine cables connect many countries, and with each connecting country hosting one or many landing stations. Some of these landing stations operate as intelligence-gathering stations, such as those in Oman. The UK's intelligence agency uses the Oman stations to gather intelligence from the Middle East and surrounding regions

(Write et al. 2013). The cables are either privately owned or by consortiums. Among the owners are Western tech companies, such as Facebook, Google, Microsoft and Amazon, which according to media reports, also assisted NSA and GCHQ to tap into the submarine cables (Zimmer 2018; Gallagher and June 2018; Greenwald 2014). According to Gallagher and June (2018), most Internet data passes through the US for two reasons. Firstly, the US sits between Europe, the Middle East, and Asia and secondly, the world's dominant Internet providers are US tech companies (The Intercept, 2018). This situation provides the NSA with ample time and opportunity to engage in digital data colonialism, which is only possible because of the Foreign Intelligence Surveillance Act (FISA) that allows the US government's intelligence agency to gather foreign intelligence by using electronic surveillance (Congressional Research Service 2020).

Intelligence Agencies and Coloniality in Southeast Asia

Most of the news stories on digital data colonialism concerned the US and the UK, but the Snowden leaks also shed light on how the Five Eyes and SIGINT Senior Pacific networks operate in the Asia and Pacific regions (Snowden 2007).

According to the Snowden leaks, as reported in The Sydney Morning Herald, Singapore, a SIGINT Senior Pacific network member, assisted both the US and Australia to spy on Malaysia and Indonesia (Dorling 2013, 2014). The leaks caused tension between the Southeast Asian neighbours and Malaysia and Indonesia on the one hand and Australia (ABC 2013). The Snowden leaks also revealed that Indonesia had been a long term target of Australia's intelligence agency, and the country used its diplomatic posts in Asia to intercept phone calls and data as part of the Five Eyes digital data colonialism efforts (MacAskill and Taylor 2013; Dorling 2013; Walsh et al. 2015). According to the Snowden leaks, Australia's intelligence agency penetrated the Indonesian communication network (Indosat and Telkomsel), spied on Indonesian politicians to assist other Five Eyes members, such as the US and New Zealand (Dorling 2014; Beckford 2015). In the US's case, Australia's Signals Directorate monitored communication between Indonesia and the US law firm representing Indonesia in trade disputes with the US (The New York Times 2014). As for New Zealand, its intelligence agency, GCSB used the XKEYSCORE Internet surveillance system to collect communications about the WTO director-general candidates because the country wanted its candidate, Trade Minister Tim Groser to win. New Zealand was able to gain access to the system because it is a member of the Five Eyes. However, GCSB's main target was Mari Elka Pangestu, Indonesia's WTO director-general candidate, because New Zealand did not want an Indonesian appointed to the position (Gallagher and Hager 2015). Other candidates that New Zealand collected information on through XKEYSCORE were (Ghana); Amina Mohamed (Kenya); Anabel González (Costa Rica); Herminio Blanco (Mexico); Taeho Bark (South Korea); Ahmad Thougan Hindawi (Jordan); and Roberto Carvalho de Azevêdo (Brazil) (Gallagher and Hager 2015). There are many ways to read this situation, especially the targeting of Mari Elka Pangestu, but one thing is clear, all the targets are from non-Western countries.

The intelligence-gathering efforts by the Five Eyes and Seniors Pacific members, headed by Australia is probably one of the main reasons why Indonesia sought to establish a strategic alliance with the US by proposing an initiative called 'Our Eyes' involving ASEAN countries: Indonesia, Thailand, Malaysia, Brunei, Singapore and the Philippines (French and Agnes 2018). This initiative is not likely to become a reality for several reasons. Firstly, Indonesia is the largest Muslim majority country in the world and is seen as a breeding ground for extremism by Five Eyes and Seniors Pacific members. As such, it needs to be securitised. Secondly, the Indonesian archipelago has vast natural resources reserves, which means business opportunities for Western corporations. Thirdly, the Indonesian archipelago has enormous potential for Western tech companies to grow because of the size of the population. Finally, and perhaps the most important reason why sharing intelligence with Indonesia would be counterintuitive for the Five Eyes, and Seniors Pacific members is because of their political and economic interests.

Asian countries, specifically Southeast Asian Muslim countries, are susceptible to having their digital data colonised because of the submarine cable called: SEA-ME-WE 3 (Dorling 2013).

The cable runs from Perth, Australia, passing Indonesia, Malaysia, Singapore and Oman. The cable connects thirty-nine countries, with thirty-three of them having landing stations and covers four continents, and it is the most extended submarine cable (Submarine Networks 2020). A consortium of telecom corporations owns the cable, including Singapore's SingTel Optus, a British telecom company called British Telecom and Telstra, an Australian telecom company, which allows them to access digital data from the cable (SeaMeWe-3 2020; Dorling 2013). However, not every country has the technology to tap into the cable, as Pakistan's example illustrates (Guardian 2015). In Singapore's case, Dorling (2013) notes that the country has the most advanced signals intelligence capabilities in Southeast Asia and has facilitated access to the data running through the cable to Australia. Moreover, by tapping into the cables, powerful Western countries' intelligence agencies can colonise a vast amount of digital data during the different stages of the data's journey from sender to receiver. This data can be used for all sorts of activities that fit the economic and political agendas of powerful Western countries, like the US, UK, Australia and New Zealand cases exemplify.

Conclusion

The paper took up the modest task of discussing how the intelligence agencies of powerful Western countries and their allies engage in digital data colonialism to maintain non-Western countries' coloniality. The process of digital data colonialism involves tapping into submarine cables that criss-cross the world carrying Internet and other communication digital data. Having access to this digital data enables powerful Western countries to securitise non-Western countries and gain a political and economic advantage over them. This situation maintains coloniality and provides powerful Western countries to be omnipresent, similar to the God-Eye view, leading to dystopia.

The situation mentioned above raises several issues for scholars interested in the coloniality of non-Western countries to research. Researching these issues will also help scholars to think about how to end the coloniality of non-Western countries. Firstly, scholars need to ask Western tech companies whether they share the digital data they have colonised from non-Western countries with anyone? This question leads to two other sub-questions. (1) Do Western tech companies share the digital data with powerful Western countries, non-Western governments or neither? (2) If Western tech companies share the data with the countries mentioned above, scholars need to ask the countries about how this digital data is being used?

Secondly, scholars need to ask why the intelligence agencies of powerful Western countries are colonising the digital data produced by non-Western countries? This question leads to two other connected questions that need to be asked. (1) How do the intelligence agencies of powerful Western countries engage in digital data colonialism? (2) Do the intelligence agencies of powerful Western countries engage in digital data colonialism to further their political and economic interests in non-Western countries, like Indonesia?

Thirdly, scholars need to ask questions about 'terror capitalism' and whether the intelligence agencies of powerful Western countries and Western tech companies are using the digital data that they have colonised from non-Western countries to create pathologies and develop technology that is useful to predict who will become an extremist and terrorist. In a similar way to what the Israeli company called Faception is offering?

Fourthly, scholars need to develop tools to educate non-Western populations about digital data colonialism by tech companies and powerful Western countries' intelligence agencies. Fifth, scholars need to pressure non-Western governments to implement stringent and effective data protection legislation to prevent digital data colonialism. Finally, scholars need to pressure non-Western governments to be more vigilant about Western countries tapping into submarine cables and their data hacking practices.

Acknowledgement

I would like to thank my Colleagues at the Department of Sociology, Social Policy and Criminology, School of Law and Social Justice, University of Liverpool in United Kingdom and Singapore for the completion of this article.

References

Alatas, H. 2000. Intellectual Imperialism: Definition, Traits, and Problems. Southeast Journal of Social Science. (28)1. p23-45.

Available from: https://www.theage.com.au/technology/australian-spies-in-global-deal-to-tap-undersea-cables-20130828-2sr58.html (accessed 13th December, 2020)

Babuta, A. Oswald, M, and Janjeva, A. 2016. Artificial Intelligence and UK National Security Policy Considerations. RUSI, April.

Balce, N. 2016. Body Parts of Empire Visual Abjection, Filipino Images, and the American Archive. Michigan: University of Michigan Press.

Ball, J. 2013. NSA monitored calls of 35 world leaders after US official handed over contacts. The Guardian, October 24.

Baz, G. 2019. Artificial or Human: A New Era of Counterterrorism Intelligence? Studies in Conflict & Terrorism. (42) 12.

Bhambra, G. Nisancioglu, K. and Cebrial, D. 2018. Decolonising the University. London: Pluto Press.

Byler, D. and Boe, C. 2020. Tech-enabled 'terror capitalism' is spreading worldwide. The surveillance regimes must be stopped. The Guardian, July 24. Available from: https://www.theguardian.com/world/2020/jul/24/surveillance-tech-facial-recognition-terror-capitalism (accessed 12th December, 2020)

Coleman, D,. 2018. Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws. Michigan Journal of Race and Law. (24) 2.

Comber, L,. 2008. Malaya's Secret Police 1945–60 The Role of the Special Branch in the Malayan Emergency. Melbourne: Monash University Press.

Congressional Research Service. 2020. Available from: https://fas.org/sgp/crs/intel/IF11451.pdf (accessed 12th December, 2020)

Connell, R,. 2007. Southern Theory. London: Polity Press.

Couldry, N. and Mejias, U,. 2019. The Costs of Connection: How Data Is Colonising Human Life and Appropriating It for Capitalism (Culture and Economic Life) 1st Edition. California: Stanford University Press.

Davenport, T. 2015. Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis. Catholic University Journal of Law and Technology. (24), 1.

Digital Methods Initiative, 2020. The Webs. Available from: https://wiki.digitalmethods.net/Digitalmethods/TheWebs (accessed 12th December, 2020).

Doffman, Zack,. 2019. Facebook Has Just Been Caught Spying On Users' Private Messages And Data. Forbes, January 30. Available from: https://www.forbes.com/sites/zakdoffman/2019/01/30/facebook-has-just-been-caught-spying-on-users-private-messages-and-data-again/#7dfeec6731ce (accessed 14th December, 2020)

Dorling, P,. 2013. Australian spies in global deal to tap undersea cables. The Sydney Morning Herald, August 29.

Dorling, P,. 2013. Exposed: Australia's Asia spy network. The Sydney Morning Herald, October 31. Available from: https://www.smh.com.au/politics/federal/exposed-australias-asia-spy-network-20131030-2whia.html (accessed 13th December, 2020).

Dorling, P,. 2013. Singapore, South Korea revealed as Five Eyes spying partners. The Sydney Morning Herald, November 25. Available from: https://www.smh.com.au/technology/singapore-south-korea-revealed-as-five-eyes-spying-partners-20131124-2y433.html (accessed 13th December, 2020).

Dorling, P,. 2014. Edward Snowden documents show Malaysia is an Australia, US intelligence target. The Sydney Morning Herald, March 30. Available from: https://www.smh.com.au/world/edward-snowden-documents-show-malaysia-is-an-australia-us-intelligence-target-20140330-zqonc.html (accessed 13th December, 2020).

Dorling, P,. 2014. Edward Snowden leak: Australia spied on Indonesian phones and data. The Sydney Morning Herald, February 17. Available from: https://www.smh.com.au/politics/federal/edward-snowden-leak-australia-spied-on-indonesian-phones-and-data-20140216-32tux.html (accessed 14th December, 2020).

Faception,. 2020. Faception. Available from: https://www.faception.com/our-technology (accessed 13th December, 2020).

Fisher, M,. 2013. A staggering map of the 54 countries that reportedly participated in the CIA's rendition program. Washington Post. Available from: https://www.washingtonpost.com/news/worldviews/wp/2013/02/05/a-staggering-map-of-the-54-countries-that-reportedly-participated-in-the-cias-rendition-program/ (accessed on 11 March, 2021)

French, F. and Agnes, A 2018. Indonesia, US up the ante on counter-terrorism. Jakarta Post, January 24.

Gallagher, R,. 2018. The Powerful Global Spy Alliance You Never Knew Existed. The Intercept, March 2. Available from: https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/ (accessed 13th December, 2020).

Gallagher, R. and Hager, N,. 2015. New Zealand Spied on WTO Director Candidates. The Intercept, March 23. Available from: https://theintercept.com/2015/03/22/new-zealand-gcsb-spying-wto-director-general/ (accessed 13th December, 2020).

Gallagher, R. and Henrik, M,. 2018. The Wire Trap Rooms. The Intercept, June 25. Available from: https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/ (accessed 12th December, 2020).

Giosue, L,. 2019. Fourteen Eyes surveillance alliance explained. Jerusalem Post, June 3. Available from: https://www.jpost.com/special-content/fourteen-eyes-surveillance-alliance-explained-591436 (accessed 13th December, 2020).

Gordon, R,. 2016. How the US Military Came to Embrace Extrajudicial Killings. The Nation, July 18. Available from: https://www.thenation.com/article/archive/how-the-us-military-came-to-embrace-extrajudicial-killings/ (accessed on 3 February, 2021)

Greenwald, G,. 2014. No Place to Hide, Edward Snowden, The NSA and The Surveillance State. London: Penguin.

Greenwald, G. and MacAskill, E,. 2013. NSA Prism program taps in to user data of Apple, Google and others. The Guardian, June 6.

Grosfoguel, R,. 2013. Decolonising Post-Colonial Studies and Paradigms of Political-Economy: Transmodernity, Decolonial Thinking, and Global Coloniality. TRANSMODERNITY. (1), 1.

Grosfoguel, R,. 2013. The Structure of Knowledge in Westernized Universities: Epistemic Racism/Sexism and the Four Genocides/Epistemicides of the Long 16th Century. Human Architecture: Journal of the Sociology of Self- Knowledge. (11), 8. p9-22.

Grosfoguel. R,. 2006. World-Systems Analysis in the Context of Transmodernity, Border Thinking, and Global Coloniality. Review (Fernand Braudel Center), From Postcolonial Studies to Decolonial Studies: Decolonising Postcolonial Studies. (29), 2. p167-187.

Grosfoguel. R,. 2016. What is Racism? The Journal of World Systems Research. (22), 1. p9-15.

Hack, K,. 1999. 'British intelligence and counterinsurgency in the era of decolonisation: The example of Malaya'. Intelligence and National Security. (14), 2. p124-155.

Hack, K,. 2009. 'The Malayan Emergency as Counter-Insurgency Paradigm'. Journal of Strategic Studies. (32), 3. p383-414.

Herman, E. and O' Sullivan, G,. 1989. The Terrorism Industry: The Experts and Institutions that shape our view of Terror. New York: Pantheon Books.

Huggler, J,. 2017. Facial recognition software to catch terrorists being tested at Berlin station. The Telegraph, August 2.

Kachamas, P. Akkaradamrongrat, S. Sinthupinyo, S. and Chandrachai, A. 2019. Application of artificial intelligent in the prediction of consumer behavior from facebook posts analysis. International Journal of Machine Learning and Computing. (9), 1. p91-97.

Karari, P,. 2018. Modus Operandi of Oppressing the "Savages": The Kenyan British Colonial Experience. Peace and Conflict Studies. (25), 2.

Kaurin, D,. 2019. Data Protection and Digital Agency for Refugees. Centre for International Governance Innovation, May 15. Available from: https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees (accessed 12th December, 2020)

Komer, R,. 1972. The Malayan Emergency in Retrospect Organization of a Successful Counterinsurgency Effort. California: Rand.

Kwet, M,. 2019. Digital colonialism is threatening the Global South. Aljazeera, March 13. Available from: https://www.aljazeera.com/indepth/opinion/digital-colonialism-threatening-global-south-190129140828809.html (accessed 12th December, 2020)

Kwet. M,. 2019. Digital colonialism: US empire and the new imperialism in the Global South. Race & Class. (60), 4.

MacAskill, E. and Taylor, L,. 2013. NSA: Australia and US used climate change conference to spy on Indonesia. The Guardian, November 2. Available from: https://www.theguardian.com/world/2013/nov/02/nsa-australia-bali-conference-spy-indonesia (accessed 12th December, 2020).

MacAskill, E. Borger, J. Hopkins, N. Davies, N. and Ball, J,. 2013. GCHQ taps fibre-optic cables for secret access to world's communications. The Guardian, June 21.

Available from: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (accessed 12th December, 2020).

Maldonado-Torres. N,. 2007. On the Coloniality of Being Contributions to the development of a concept. Cultural Studies. (21), 23. p240-270.

Marczak, B. Scott-Railton, J McKune, S. Abdul Razzak, B. and Deibert, R,. 2018. HIDE AND SEEK Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. Citizen Lab, September 18. Available from: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/ (accessed 12th December, 2020)

McKendrick, K,. 2019. Artificial Intelligence Prediction and Counterterrorism. Chatham House, The Royal Institute of International Affairs. Available from: https://www.chathamhouse.org/sites/default/files/2019-08-07-AICounterterrorism.pdf (access 12th December, 2020)

Mejias, U. and Couldry, N,. 2020. Resistance to the new data colonialism must start now. Aljazeera, April 29.

Mignolo, W,. 2011. The Darker Side of Western Modernity: Global Futures, Decolonial Options. North Carolina: Duke University Press.

Monique, M. and Angela, D,. 2019. (Big) Data and the North-in-South: Australia's Informational Imperialism and Digital Colonialism. Television & New Media. (20), 4. p379-395.

Mwambari, D,. 2020. The pandemic can be a catalyst for decolonisation in Africa. Aljazeera, April 16.

Ndlovu-Gatsheni, S,. 2013. Coloniality of Power in Postcolonial Africa. Oxford: African Books Collective.

Notias, T,. 2020. Access granted: Facebook's free basics in Africa. Media, Culture & Society. (42), 3. p329-348.

O'Neil, A. 2017. Australia and the 'Five Eyes' intelligence network: the perils of an asymmetric alliance. Australian Journal of International Affairs. (71), 5. p529-543.

Pfluke, C,. 2019. A history of the Five Eyes Alliance: Possibility for reform and additions. Comparative Strategy. (38), 4.

Pinto, R,. 2018. Digital Sovereignty or Digital Colonialism? Revista International de Direitos Humanos. (15), 27.

Quijano, A. 2007. Coloniality and Modernity/Rationality. Cultural Studies. (21), 23. p168-178.

Raphael, S; Black, C; Blakeley, R; Kostas, S. 2016. Tracking rendition aircraft as a way to understand CIA secret detention and torture in Europe. International Journal of Human Rights. (20) 1. p78-103.

Richelson, J. 2012. The US Intelligence Community. 6th ed. Boulder. Colorado: Westview Press.

Said, E,. 1978. Orientalism. New York: Vintage Books Edition.

Santander, P,. 2010. Latin America: Political communication and media discourse in contexts of social and revolutionary transformations. Journal of Multicultural Discourses. (5), 3. p227-238.

Santos, B,. 2014. Epistemologies of the South Justice against Epistemicide. London: Routledge.

Santos, B,. 2018. The end of the Cognitive Empire, the coming of age of epistemologies of the south. North Corallina: Duke University Press.

SeaMeWe-3,. 2020. Fiber Atlantic. Available from: http://www.fiberatlantic.com/system/xk14q (accessed 12th December, 2020).

Snowden, E. 2007. SIGINT Seniors Pacific. March 16. Available from: https://edwardsnowden.com/wp-content/uploads/2018/06/SIDtoday-2007-03-16-SIGINT-Seniors-Pacific.pdf (accessed 12th December, 2020).

Snowden, E. 2007. The Courage Foundation, March 16. Available from: https://edwardsnowden.com/2018/06/01/sigint-seniors-pacific-successes-highlighted-at-conference/ (accessed 12th December, 2020).

Solon, O,. 2017. It's digital colonialism': how Facebook's free internet service has failed its users. The Guardian, July 27. Available from: https://www.theguardian.com/technology/2017/jul/27/facebook-free-basics-developing-markets (accessed 12th December, 2020).

Stampnitzky, L,. 2014. Disciplining Terror, How Scholars Invented Terrorism. Cambridge: Cambridge University Press.

Steinmetz, G,. 2017. Sociology and Colonialism in the British and French Empires, 1945–1965. The Journal of Modern History. (89), 3.

Submarine cable maps, 2020. TeleGeography. Available from: https://www.submarinecablemap.com (accessed 13th December, 2020).

Submarine. 2020. Submarine networks. Available from: https://www.submarinenetworks.com/en/stations (accessed 14th December, 2020).

Tao, L,. 2018. Malaysian police wear Chinese startups AI camera to identify suspected criminals. South China Morning Post, April 20. Available from: https://www.scmp.com/tech/social-gadgets/article/2142497/malaysian-police-wear-chinese-start-ups-ai-camera-identify (accessed 12th December, 2020)

The Intercept, 2018. SIDtoday 2007-01-08: Counterterrorism Analytic Working Group Meets in Madrid. The Intercept. Available from: https://theintercept.com/document/2018/03/01/sidtoday-2007-01-08-counterterrorism-analytic-working-group-meets-in-madrid/ (accessed 12th December, 2020).

The Intercept. 2018. Introduction, US. as World’s Telecommunications Backbone. The Intercept. Available from: https://theintercept.imgix.net/wp-uploads/sites/1/2018/06/direct-path-1529876697.png?auto=compress%2Cformat&q=90 (accessed 12th December, 2020).

The New York Times,. 2014. Document Describes Eavesdropping on American Law Firm. The New York Times, February 15. Available from: https://www.nytimes.com/2014/02/16/us/document-describes-eavesdropping-on-american-law-firm.html (accessed 12th December, 2020).

Tuck, E. and Yang, K,. 2012. Decolonisation is not a metaphor. Decolonisation: Indigeneity, Education & Society. (1), 1.

UNHCR, 2015. Biometric Identity Management System. UN. Available from: https://www.unhcr.org/550c304c9.pdf (accessed 12th December, 2020)

Walsh, P. and Miller, S. 2015. Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden. Intelligence and National Security. (31), 3. p345-368.

Yazid, A. 2019. The Police Special Branch in Countering the Malayan Emergency 1948-1960: An Analysis of Intelligence Tactics and Strategies. Malaysian Journal of international Relations. (7), 1.

Zimmer, J. 2018. Google Owns 63,605 Miles and 8.5% of Submarine Cables Worldwide. BROADBAND NOW, September 12. Available from: https://broadbandnow.com/report/google-content-providers-submarine-cable-ownership/ (accessed 16th December, 2020).

Zuboff, S. 2019. Surveillance Capitalism. New York: Hachette Book Group.