Routledge
Taylor & Francis Group

Australian Journal of International Affairs

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/caji20

Understanding the risks of China-made CCTV surveillance cameras in Australia

Ausma Bernot & Marcus Smith

To cite this article: Ausma Bernot & Marcus Smith (2023): Understanding the risks of China-made CCTV surveillance cameras in Australia, Australian Journal of International Affairs, DOI: 10.1080/10357718.2023.2248915

To link to this article: https://doi.org/10.1080/10357718.2023.2248915

Published online: 24 Aug 2023.

AUSTRALIAN JOURNAL OF INTERNATIONAL AFFAIRS
https://doi.org/10.1080/10357718.2023.2248915

Routledge
Taylor & Francis Group

Understanding the risks of China-made CCTV surveillance cameras in Australia

Ausma Bernot [a] and Marcus Smith [b]

[a]Australian Graduate School of Policing & Security, Charles Sturt University, Canberra, Australia; [b]Center for Law and Justice, Charles Sturt University, Canberra, Australia

ABSTRACT

In the global interconnected economy, China-made information-collecting technologies such as closed-circuit television (CCTV) surveillance cameras have become popular products for routine video-based surveillance. Hikvision and Dahua are the two largest global suppliers of CCTV cameras, with both companies supplying their products to over 200 countries. Despite their popularity, national security concerns are commonly cited when adopting these cameras, citing manufacturer links with the Communist Party of China (CPC), cybersecurity vulnerabilities, and sales recorded in the Xinjiang region, that has records of human rights violations. This paper is structured in three parts: first, we explore the predominance of China-made information-gathering technologies in Australia; second, we summarise common national security concerns usually associated with China-based technology manufacturers; and third, we propose regulatory measures to regulating China-made CCTV cameras in Australia. The paper suggests that while state and Federal decision-makers are free to remove Chinese CCTV surveillance cameras, they should avoid overt politisation. Overall, a stronger focus should be placed on evaluating cybersecurity risks of Internet of Things (IoT) information-collecting technologies and considering their timely and effective regulation from the perspective of individual and national interests.

KEYWORDS

surveillance; national security; CCTV; China's Party–state; privacy; data security; IoT

Introduction

In February 2023, Australia entered a public debate on whether Federal Government agencies should be using China-made CCTV surveillance cameras from Dahua and Hikvision. Such concerns mirrored debates in the United States (US), the United Kingdom (UK), and the European Union. The debate began when a media release by Australia's Shadow Cybersecurity Minister's audit concluded that over 900 Chinese-made surveillance cameras from Dahua and Hikvision were being used in Federal agencies. The media release cited the UK Government Biometrics and Surveillance Camera Commissioner calling China-made cameras 'digital asbestos,' and pointed to removal actions

CONTACT Ausma Bernot abernotaite@csu.edu.au

taken by Australia's strategic allies—the United States and the United Kingdom (Paterson 2023). Shortly after, several Australian government agencies, Federal and state, committed to removing the cameras from government buildings (Vinall 2023). Apart from their China-made origin and the companies' prior sales record to Xinjiang, the North-Western region of China where the United Nations recently reported serious human rights violations, the audit did not comment on any technical details of the cameras, such as device models, internet connectivity, facial recognition capabilities, or prior cybersecurity vulnerability concerns. Such omissions miss an opportunity to raise broader regulatory concerns about information-collecting[1] technologies, as we argue in the third section of this paper.

IoT devices connect to wireless internet networks and have data collection, storage, and transfer capabilities. The CCTV cameras that are widely marketed on the websites of both Hikvision and Dahua can potentially be linked to the internet. For example, one of Hikvision's surveillance cameras offer 'flashing lights and audible warning' and a focus on human and vehicle targets 'based on deep learning' (Hikvision n.d.). Similarly, Dahua devices offer real-time facial recognition and descriptive statistics of the faces captured, including 'age and gender distribution' (Dahua n.d.). While such IoT cameras provide more functions, they also have increased cybersecurity risks, commonly through use of default login details, manufacturer vulnerabilities, and hacking (Gavrovska and Samčović 2020). Simon (2017) outlines four main types of cyber-attacks commonly linked to IoTs, increasing in impact severity: 'hacktivism,' cybercrime, cyber-espionage, and cyberwar. Internet-connected infrastructure has thus given rise to 'promise vs. peril' debates in government and academia relating to the interdependence of critical infrastructure and IoT devices (Simon 2017).

CCTV cameras are now commonly produced as IoT devices: among other functions, IoT CCTV cameras often have automated alerts, can be set to record video streams, and can stream video online allowing their users to monitor real-time footage. IoT CCTV cameras contain more functions, such as remote surveillance, facial recognition, and even demographic statistics, but they also create more technical vulnerabilities. Due to a lack of 'strategic trust' between Australia and China (Hartcher 2021), concerns about the potential to engineer vulnerabilities into the hardware or software of IoT CCTV cameras have been raised at the levels of Federal and state governments. Australia's narrative of 'strategic trust' (or lack thereof) in China links to geo-economics—'an interplay of international economics, geopolitics, and strategy' (Hussain 2021).

National security is central to the issues discussed in this article. We adopt the following definition:

> [National security is the] measurable state of the capability of a nation to overcome the multi-dimensional threats to the apparent well-being of its people and its survival as a nation-state at any given time, by balancing all instruments of state policy through governance … and is extendable to global security by variables external to it. (Paleri 2008, 54)

The national economy is often linked to national security conceptions—a key theoretical concept that ties the empirical contributions of this article. As James G. Rickards (2009) observed, national security can be 'captive' to economic security, inescapably tying the two together, even though economic security is not explicitly recognised as national security by the Federal government (Australian Government n.d.). China is Australia's

largest trading partner and one that is likely to react coercively to any politicised trade restrictions (Ferguson and Lim 2021). Indeed, following Australia's CCTV inquiries, the Chinese Foreign Ministry spokesperson Mao Ning called for fair market competition for Chinese companies by saying that 'the Chinese government always encourages Chinese companies to engage in international investment and cooperation in accordance with market principles, international rules and local laws'; She also called for business neutrality by expressing strong opposition to Australia 'over-stretching the concept of national security and abusing state power to discriminate against and suppress Chinese companies' (Ministry of Foreign Affairs of the PRC 2023).

Globalisation, national security and economy are increasingly tied together. Dupont and Reckmeyer (2012, 34) recommend that the Australian government should develop a comprehensive approach to evaluating security challenges, and not treat them 'as independent, compartmentalised issues.' This article uses the analytical study of China-made CCTV surveillance cameras manufactured by Dahua and Hikvision to illustrate how a more comprehensive approach by the Australian government is needed to evaluate imported technologies and their data privacy and security risks. A 'whack-a-mole' approach to China-made technologies, as Bennett Moses (2023) argues, politicises government narratives and does not provide appropriate national security protections for Australians. For example, the Australian market is not only supplied by Dahua and Hikvision CCTV cameras, but also cameras from other Chinese manufacturers with lower market shares, such as Concord or Eufy. IoTs produced by other countries also carry data collection and espionage risks (Bernot 2022). Additionally, the economic element to politicised national security risks may hurt Australia's economy more than it would China's because—China diversifies its imports a trade security element that vulnerable Australian industries are currently encouraged to strengthen (Ferguson and Lim 2021).

By 2018, Australians were estimated to have purchased 16 million IoT devices (Australian Research Council 2020), and the total IoT market was evaluated as worth almost A $19 bn that year, a large portion of which are produced in China, with an estimated annual market growth of 14% (PwC 2018). Responding to the growing numbers of IoT devices in Australia, the Government has placed an increasing focus on governing their production and use. For example, in 2020, the Australian Government introduced a 'Voluntary Code of Practice: Securing the Internet of Things for Consumers' based on consultations with the Department of Home Affairs and the Australian Signals Directorate (Chalmers 2022). Before Australia builds native IoT manufacturing industries, diversifies its trade routes, and drafts clear regulation to govern IoT manufacturing and supply, security concerns related to IoTs will remain.

This paper addresses those concerns in terms of the Chinese surveillance cameras used by the Australian Government and proposes a way to mitigate national security risks. To that end, we aim to explain the key concerns of Australians' CCTV data access from China and review the legal and regulatory measures required to preserve the privacy and security of Australians' data potentially linked to CCTV cameras. This article is an interdisciplinary contribution that draws on Chinese security studies and Australian regulation scholarship to analyse a contemporary issue in Australian politics. We have integrated sources from Dahua, Hikvision, and policy makers, where available, and supplemented those sources with scholarly and grey literature to support our critical scholarly interrogation.

The first aim formulates the data access concerns and contextualises them in the political–legal context of China, including the 'authoritarian capitalist dynamic' (Huang and Tsai 2022, 2) to which China-based companies are bound. The second aim maps Australia's current regulatory capability to respond to those concerns. The article progresses in three parts: first, we discuss the application of China-made information-collecting technologies in Australia. Next, the article explains the political and legal context of private technology manufacturers from China, including their national security obligations to the Party–state (Australian Research Council 2020). The third part of the article draws from the first two parts to suggest the actions that the Australian Government should consider in regulating information-collecting technologies manufactured in China.

The key argument analyses the balance of national security and economic interests between Australia-China and Australia's increasing governance focus on data security, to argue that clearer Federal regulation is key to managing the use of China-made IoT devices in Australia. It is not sufficient to point to the national origin of information-collecting technologies. Rather, a more nuanced and clear regulatory position needs to be taken by Australian Government actors in articulating the actual and potential threats of such technologies. Additionally, the Australian government should consider the broader regulatory expectations for technology companies that would legally bind the companies to responsible data management practices.

Context of information-collecting Chinese technologies in Australia

Concerns regarding information-collecting technologies fully or partially manufactured in China are here to stay as Australia is reliant on China for the supply of these technologies. Due to the lack of information technology regulations, they are also likely to re-emerge every time a new technology application reaches the Australian market. This section highlights the debates about several of such technologies—IoT CCTV cameras, TikTok, iPhones, and 5G, the use of which the Australian Government contested in August 2018 (Hartcher 2021). The concerns of data misuse are likely to be similar, only appearing in the form of different emergent technologies.

China is Australia's most important trading partner, accounting for 39% of all goods exported in 2019–2020 and 27% of all commodities purchased (Australian Bureau of Statistics 2020). In August 2022, following trade disputes with China (Miller 2022), Australia's imports from China paradoxically hit a record high of A$10.6 billion—larger than the United States, the United Kingdom, and Japan combined in that month (Mizen 2022). The imports coming in from China are not only low-value labour-intensive goods: in 2019–2020 the third of all imported products were telecommunication and sound equipment, office and automated data processing machinery, electrical machinery and appliances (Australian Bureau of Statistics 2020). In 2015, the Xi Jinping administration proposed a 10-year plan 'Made in China 2025' that aims to move China's manufacturing to 10 higher-value industries, including new information technologies, high-end machines and robots, aerospace equipment, and electrical equipment (The State Council of the PRC 2015). Since 2015, China's government has heavily invested in these target areas, including support for Internet of Things (IoT), cloud computing, and artificial intelligence companies (Gao 2019).

The trade relations between Australia and China are closely intertwined. From CCTV cameras to 5G infrastructure and the collection of genetic data, the Australian Government authorities are bound to continue running into the repeated issues of Chinese companies' potential for collecting or allowing access to Australians' data in China. In 2021, independent researchers surveyed Shodan—a global search engine of internet-connected devices—and found that Australia houses over 60,000 Hikvision and Dahua surveillance camera networks—over 41,000 from Hikvision and 18,000 from Dahua (Migliano and Woodhams 2021). The number is small in comparison. The two companies have over 700,000 camera networks in the United States and over 800,000 in Vietnam. The 900 cameras on Federal buildings identified in Australia's February audit constitute only a small portion of the total number of cameras installed in Australia. In encouraging the removal of Hikvision and Dahua cameras, three core concerns were raised by Australian government representatives: the companies' links with the Chinese Party–state, their sales records in Xinjiang region, and concerns about potential data access from China (Paterson 2023).

Other information-collecting technologies have had similar concerns raised in Australia. Since 2020, Australian Government actors have also been looking at data transfer and access concerns around the use of the social media app TikTok, which reported 7 million users in Australia in September 2022 and revenue of A$71.8 million (US$50 million) in 2021 (Mason 2022). In June 2022, Buzzfeed published a report based on 80 leaked internal TikTok meetings (Baker-White 2022). The report confirmed that while data in the US is not actively transferred to China, it can be *accessed* in China via access permissions to cloud-based data servers. At the time of writing, the Australian Federal Government is undergoing a review of cybersecurity implications of all social media use in the public service and government departments. In April 2023, Australia's Attorney-General issued a statement banning TikTok from Federal government devices (Bonyhady and Knott 2023), and the app has been banned on government work phones in the United Kingdom (Geiger and Kleinman 2023), United States (Shepardson 2023), and the European Union (Xu, Brennan, and Frater 2023).

Several other examples of China-made technologies mirror the theme of data concerns. BGI (Shenzhen Huada Gene Technology Co. Ltd; 深圳华大基因科技有限公司), a genomics company that had data security concerns raised about genomic data derived from prenatal testing kits, Non-Invasive Fetal TrisomY (NIFTY), that capture genomic data from the pregnant person tested and the foetus (Needham and Baldwin 2021). In addition, in August 2018 Australia became one of over twenty countries to ban Huawei's 5G infrastructure from entering public tenders because the company was deemed likely to 'be subject to extrajudicial directions from a foreign government' (BBC News 2018).

The below section articulates key concerns related to Australia's 'China challenge discourse' (Laurenceson 2018) and contextualises them in China's political–legal background.

Concerns linked to China-based technology manufacturing

National security interests are increasingly shaping economic policies and decision-making (Golley *et al.* 2020). The debates about economic globalisation tie national

economics and security together by emphasising great-power competition, strategic rivalry, security concerns, and ideological conflict as its central factors (Roberts and Lamp 2021). In considering Chinese-made technologies, Australia lacks 'strategic trust' towards China (Hartcher 2021). At the forefront of national debates about information-collecting technologies made by China-based manufacturers, three areas of concern are considered—Chinese technology company links with the Party–state, legal data transfer obligation under the Chinese law, should such transfer be requested, and technical vulnerabilities—accidental or by design. These two concerns undergird further considerations, such as national and cyber security risks (Hartcher 2021) and potential impacts on critical infrastructure vulnerabilities such as communications networks linked via space (Schaefer 2018) or submarine cables (McGeachy 2022). The next three sections expand on the source of concerns around public-private partnerships and data transfer obligations and contextualise them within China's political developments.

Chinese technology company links with China's Party–state

The Chinese government is a large buyer of emergent technologies such as Artificial Intelligence, biotechnology, and cybersecurity products. Huang and Tsai (2022, 2) argue that autocratic countries are forced to rely on foreign suppliers or allow local private businesses to enter the vital industrial sector to establish a powerful surveillance state and call this an 'authoritarian capitalist dynamic.' It is this dynamic that helps China's Party–state to merge the social control interests of the Party–state and profit-seeking interests of private enterprise. Additionally, the Party has control over the administration of the state, the two being inseparable in China. It is therefore reasonable to expect that most large private companies are affiliated with the Chinese Party–state to some extent. This section explains those intertwined interests between the CPC, the state, and private actors.

Since the late 1970s when China's market opened up to capitalist trade within China and internationally, profit-seeking behaviours have motivated not only China-based start-ups but also international companies. Following international collaborations and the eventual growth of domestic technology providers (Bernot 2022), China's market system eventually evolving into 'party–state capitalism'—a political economy undergirded by the aims to maintain continued ownership of political power by the CPC (Pearson, Rithmire, and Tsai 2022).

Targeting the Party–state as a buyer not only has direct sales benefits. It is not surprising that Chinese technology companies are keen to align themselves with the strategic goals of the Chinese Party–state, considering that the Chinese market offers sustained financial benefits, domestic and international competitiveness-building advantages, and occasionally even promotes Chinese technologies via political alliances (Bernot 2022). In a recent publication Trevaskes and Bernot (2023, 3) showcased promotional materials from Hikvision and three smaller surveillance technology companies and argued that 'ideological concepts … undergird the links between the Party–state and surveillance company products and services.' The article highlights how these four companies use government documents to align their business goals with the national political and ideological strategies of the Party–state. In one particularly striking example, the

authors cite a Hikvision spokesperson promoting an integrated video surveillance and facial recognition product 'Sharp Eyes' by describing the technology as 'an important means to maintain national security and social stability, prevent and combat violent and terrorist crimes,' directly parroting official state narratives (5). Additionally, Huang and Tsai (2022, 4) noted that smaller technology companies might compete with large established technology giants by offering more intrusive and powerful information-collecting products and services. For some of the largest companies in China, aligning company goals with those of the Party–state is a long-standing business strategy, a foundation for ensuring Party–state support, such as subsidies or strategic business development (Bernot 2022).

The Party–state also takes an active approach to establishing presence in private enterprises, consolidating the motivations for private and semi-private companies to be tied to the state. Pearson and colleagues (2022) argue that China's Party–state capitalism differs from state capitalism in two main ways: first, the Party–state actively extends its presence to private enterprise via practices of corporate governance and financial instruments and second, it requires political loyalty from firms and the persons who are tied to them.

Writing to the first point, the authors highlight that by 2018, 1.88 million non-state enterprises (73%) had created Party cells (Pearson, Rithmire, and Tsai 2022, 152). Although scholarly literature considers the nuance of political influence between the Party cells and companies, such as the firms actually transmitting influence on the Party cells (Hawes 2022), the pragmatic business interests of private companies strategically link them with contested decisions taken by the Chinese Party–state. In relation to the present object of study, the Australian Strategic Policy Institute identified that both Dahua and Hikvision have close ties with the Chinese government and the Party and have supplied the surveillance infrastructure in Xinjiang: Dahua maintains active Party committees and branches, has received direct financial support from the Chinese government from national projects, an extensively supplies Xinjiang-based projects in areas of public security and 'counter-terrorism'—a political double-speak keyword for ethnic minority repression (Australian Strategic Policy Institute n.d.a); Hikvision similarly maintains active Party affiliations: some of its subsidiary companies have joint public-private ownership, the company was visited by Xi Jinping in 2015, and has contributed to surveillance infrastructure in Xinjiang, most controversially by supplying facial recognition and surveillance systems for extra-legal internment camps of ethnic minorities (Australian Strategic Policy Institute n.d.b).

The second aspect of China's Party–state capitalism is that of financialisation—investment of state-controlled capital beyond state-owned firms. State-backed financialisation often happens via state-owned capital investment companies that ascertain investment directions. Unlike privately owned investment companies, government-backed financialisation organisations can locate funds in support of private and semi-private enterprise according to both financial and political goals. This difference proved significant during the 2015 stock market crisis when state-backed investments prioritised economic stability rather than capital gains (Pearson, Rithmire, and Tsai 2022, 153).

The Party–state is proactively seeking to gauge increased political loyalty and provide financial security to companies in return. Additionally, state buying constitutes a large portion of many companies' domestic sales, helping China's government to both develop a strong market and fulfil state interests. For instance, according to the available

data from 2020, domestic Chinese companies supplied more than half of the total US $11.93 billion IaaS cloud infrastructure market in China (IDC 2021). Private companies are often financially motivated to maintain a close relationship with the Party–state, thus proactively adding to the muddling of private-state relationships.

Legal data transfer obligations to China's national security actors

Private company connections do not necessarily imply that companies share their data with the Chinese Party–state by default. It is China's legal and regulatory background that binds all companies to disclose data upon request. Specifically, following Xi Jinping's ascent to political power in 2012, a suite of new laws and regulations, exemplified below, around private company data and its sharing with state actors strengthened those obligations. The 'umbrella concerns' that seep through these laws and regulations are those of foreign interference and increased Party–state control over information-collecting technologies. This section traces the regulatory developments of state data access centralisation in China from 2013, spotlighting the regulations that could hypothetically allow China's government access to internationally collected data that is stored in and/or accessed from mainland China.

The political context of the last decade is important to understand the scope of current laws and regulations guiding information collection work. In particular, all of the key laws and regulations discussed were published by the administration of Xi Jinping, who became the leader of the Party–state in 2012. At the very beginning of his leadership term, it became clear that Xi was taking a different role of political leadership as compared to the previous China's leader Hu Jintao. Under the newly minted ideological concept of 'comprehensive national security' (总体国家安全), he expanded the scope of international risks (including cybersecurity) and called for a stricter model of governance to respond to those risks (Drinhausen and Legarda 2022).

As part of Xi's stricter strategy to both growing big data and internet industries as well as regulating them, the Xi Administration has introduced a suite of laws and regulations over the last decade (2013–2023). Namely, we address the 2014 Counterespionage Law of the PRC (中华人民共和国反间谍法) and 2017 National Intelligence Law (国家情报法) because these two Laws particularly feature in international debates on the privacy and data security risks of Chinese technologies. While outside of the scope of this paper to discuss in full, it is important to note that these laws link to a broader ecosystem of other laws, such as the 2015 National Security Law that outlined a new 'Xi-ism'—the concept of holistic national security (总体国家安全) to which national security threats are now linked (Drinhausen and Legarda 2022). These laws oblige companies established in China to closely collaborate with the government if requested.

The Counterespionage Law was adopted in November 2014 during the Twelfth National People's Congress in November. The law stresses 'mass line,' hinting at a whole-of-society approach to counter-espionage, 'active defence,' and tasks state security agencies with counter-espionage efforts. The Law largely imported its content from the previous National Security Law, but its later iterations greatly expanded the scope of the Law, specifically the 2017 Detailed Implementation Rules for the Counterespionage Law (further, Implementation Rules) and Provisions on Efforts on Counterespionage Security Precautions (further, Provisions).

Jeremy Daum (2017) remarked that the 2017 Implementation Rules allow to investigate acts of subversion that are not espionage when they are determined to be endangering national security. The Implementation Rules also increase punishment limits from refusing to disclose evidence and single out foreign citizens living in China as a group requiring heightened surveillance, among other examples of scope creep. The Provisions to the law are further published in 2021 and call on 'people's groups, enterprises, public institutions, and other social organisations to implement responsibility for counter-espionage,' adopting an all-of-society responsibility model. Overall, the Counterespionage Law now calls on individuals, groups, companies, and government organisations to proactively partake in counter-espionage and introduces penalties for refusing if engaged by authorities. This 'all-of-society' approach to intelligence collection was further consolidated in the 2017 National Intelligence Law.

National Intelligence Law is the first law that was drafted specifically for China's national intelligence agencies. Article 7 of the Law is the most contested part of the legal text, because it stipulates that:

> All organisations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of. The State protects individuals and organisations that support, assist, and cooperate with national intelligence efforts (The Standing Committee of the PRC 2017).

Article 7 not only places responsibility on all organisations and individuals within China to cooperate with intelligence gathering. The law promotes a carrots-and-sticks approach by outlining provisions for rewards and also including stipulations in case of non-compliance. Major contributions to national intelligence efforts by individuals and organisations can receive commendations and awards from the state, while obstruction of national intelligence work can result in warnings from state and public security organs, up to 15 days in detention and even criminal responsibility. In a media conversation with People's Daily, the Information Office of the Ministry of State Security stressed that 'national security is everyone's responsibility, and everyone must fulfil their responsibilities' (Fu and Qin 2021).

The Office also outlined that behaviours perceived as endangering state security can be reported by individuals via a designated hotline or reported online. Such crowdsourced intelligence reporting practices date to the Mao Zedong era when citizens were strongly encouraged to report on each other. Xi Jinping's leadership has revived numerous historical Maoist practices, including citizen-led mass reporting that is now deployed to call on 'counter-terrorism' and anti-Party–state sentiments on university campuses (Jiang 2021). Law and digital technologies play a significant role in supporting those resurrected practices.

China-based or -linked companies that operate internationally are often questioned based on the 2017 National Intelligence Law. For instance, Huawei (n.d.) officially claims to have obtained an independent legal opinion stating that the 2017 National Intelligence Law does not force the company to engage in intelligence gathering activities. Similarly, TikTok (n.d.) proposed Project Texas to store US customer data locally in the US after continued data access from China was reported in June 2022 (Baker-White 2022). However, private company compliance with national law within China's jurisdiction bears potential criminal responsibility. This legal liability has been considered a risk

by liberal democracies: In 2023, the National Cyber Security Centre (NCSC) of GCHQ, UK's key national intelligence agency, recommended a risk-based approach despite their evaluation reportedly not having revealed specific threats (Boland 2023).

State-supported media now provides some examples of intelligence reporting. In a 2021 People Daily article titled 'Acts that endanger national security may be around us' reported 'typical cases', including one on an alleged overseas spy that recruited a person on WeChat to monitor a port area in Guangdong (Xiao, Fu, and Su 2021). Future news and government articles on awards and commendations given to individuals and organisations may reveal further extent and scope of the new intelligence reporting activities.

It is reasonable to expect that the National Intelligence Law will make it difficult for organisations and individuals to resist information collection by state and public security agencies, because they can be held criminally liable for obstruction of intelligence collection. Like in Australia, it is unlikely that the cases of data transfer to national intelligence actors would be kept secret and not be publicised in company reporting documents.

Technical vulnerabilities of IoT CCTV cameras

In Australia in 2021, more than 60,000 Hikvision and Dahua CCTV surveillance cameras were estimated to be operational. With the advancement of artificial intelligence, facial recognition functions can either be integrated into IoT CCTVs or applied to video footage separately (Amin, Ahman, and Ali 2016), thus introducing another layer of personal data threats. This section highlights previous vulnerabilities and addresses the political framing of those vulnerabilities in the political context of Australia and its allied countries.

Cybersecurity vulnerabilities of Hikvision and Dahua are not hypothetical. Various vulnerability databases list both Hikvision and Dahua, amid a long list of other companies (CCTV Calculator n.d.). Although it is not uncommon for vulnerability databases to list private company products, the impact that Hikvision and Dahua have is larger than a bug that can be fixed with a company-wide announcement. Both companies are also Original Equipment Manufacturers (OEM) supplying their products to other brands, that may not be aware of newly found vulnerabilities. In 2021, Hikvision fixed a vulnerability that allowed hackers extensive access to the cameras and the network linked to the cameras both within and outside China. Despite the fix, 80,000 Hikvision camera users were found to be subject to those vulnerabilities due to not having installed a firmware update (Paganini 2022).

The lack of strategic trust between Australia and China deepens cybersecurity concerns. The cyber concerns raise questions if the vulnerabilities are accidental or created by design for purposes of espionage. A senior intelligence officer commented that 'It's the control of the design that gives you zero cost of entry [to collect intelligence]. It's a lot harder to reverse-engineer to find the malign element' (Hartcher 2021). Cyber-espionage fears are strengthened by ongoing malicious cyberattacks originating from China. In 2021, in an official announcement, Australia's then Home Affairs Minister, Karen Andrews, attributed China's Ministry of State Security to malicious cyber activities related to Microsoft Exchange software vulnerabilities (Saunokonoko 2021). Large-scale cyberattacks in Australia in 2021 and 2022 targeted information about critical

infrastructure (e.g. defence, health, government sectors), the origins of which were also attributed to China (Australian Cyber Security Centre 2022; CyberSecurity Connect 2021). From the perspective of the Australian government, attacks on critical infrastructure would be of concern in case of political conflict, as they would have the capacity for large-scale societal disruptions.

Combined with Chinese companies' connections with the Party–state, cybersecurity concerns have been mirrored across other countries that Australia maintains strategic relationships with. Indeed, the Australian Home Affairs Deputy Secretary, Mark Ablong, recently quoted strategic security alignment with the United States and the United Kingdom, noting that '[f]or the same reasons that the US and the UK have looked at these technologies, we remain concerned about those companies and their relationship with the Chinese Government' (Brookes 2022). In 2018, the US–China Economic and Security Review Commission concluded that Chinese IoT devices may reveal information that was not planned to be shared as data are aggregated and combined. Additionally, the Review Commission clearly articulated espionage concerns:

> China's central role in manufacturing global information technology, IoT devices, and network equipment may allow the Chinese government—which exerts strong influence over its firms—opportunities to force Chinese suppliers or manufacturers to modify products to perform below expectations or fail, facilitate state or corporate espionage, or otherwise compromise the confidentiality, integrity, or availability of IoT devices or 5G network equipment (US–China Economic and Security Review Commission 2018).

In November 2022, the United States' Federal Communications Commission deemed that communications equipment manufactured by Hikvision and Dahua, among other China-headquartered companies, poses a threat to national security (Federal Communications Commission 2022). The ban referenced actions taken as part of the federal government's broader effort to secure US communications networks and prohibit the use of equipment that could allow a foreign enemy to exploit those networks, without providing specific details of the threats posed by Hikvision and Dahua. The use of public funds was prohibited from purchasing equipment or services and the Government instated a reimbursement scheme to remove and replace insecure equipment that had already been installed in US networks.

The overall cybersecurity risk associated with Chinese-made CCTV surveillance cameras also more broadly applies to all IoT devices. Some of the information that is missing from conducting an actual cybersecurity evaluation concerns the types of CCTV cameras installed, the way they collect, store (e.g. on-device or online), and analyse data collected, the quality and security processes undertaken prior to the camera installation, and camera security characteristics.

Regulatory approaches to Chinese-made CCTV cameras in Australia

The potential security sensitivities associated with the use of Chinese-made CCTV cameras in Australia is the latest in an ongoing public debate in relation to both Chinese-made electronic products and digital services. Specifically, the February 2023 government audit of the number of Chinese CCTV cameras installed accelerated those debates. This development is taking place in the context of a trade dispute that escalated

following the Australian Governments comments about the origins of the COVID-19 virus and the broader geopolitical dispute in the South China Sea.

The first aspect to be addressed is the international element. If, based on technical advice, CCTV cameras can store and transmit images or other data to the Chinese state, this is obviously a concern considering the Chinese National Intelligence Law 2017, and the fact that the countries are not politically aligned. The Australian Federal Government, as well as Australian corporations undertaking work that may be associated with national security implications (e.g. national intelligence and security organisations, and other Federal agencies), could simply determine not to use Chinese-made cameras in their workplaces. The decision is not one that needs to be publicly advertised or necessarily enacted in legislation and could be achieved in a politically sensitive manner avoiding, assuming non-Chinese-made options are available. For instance, the February 2023 audit focused on counting Hikvision and Dahua cameras based on their national origin and expressed dual concerns—moral concerns over the companies' sales to Xinjiang region and data security. The measures of removing the cameras from Federal buildings do not address either of those concerns in full: first, small scale government bans are not likely to affect market opportunities that large Chinese technology companies are able to access due to technical sophistication of China-made products and a relative price advantage; second, they can address espionage risk to some extent but do not actually provide any substantive cybersecurity evaluation of cameras adopted.

In the present case and to the extent of information that the Government audit revealed, CCTV cameras only pose a risk if they are used in sensitive environments such as Federal government buildings, and a different approach may, therefore, be appropriate to mitigate the lesser risk they present. In both instances, it is unclear why this would need to be publicly discussed: presumably the government could use non-Chinese-made products and state that the decision was made based on commercially sensitive reasons that are not required to disclose—a practice commonly used by Australian Federal Government agencies. The fact that these issues are being highlighted by conservative opposition politicians, who also publicly canvass the prospect of war with China, may be an indication of political motives. More broadly, overt politisation of China-made technologies ignores the pressing issue of IoT under-regulation (Harkin, Mann, and Warren 2022) and the rising ease with which face recognition technology applications may be used (Mann and Smith 2017).

The decision of the National Security Committee of Cabinet in August 2018, to ban Huawei from providing infrastructure for Australia's 5G network, is a precedent that should be noted as having potentially set a path dependency for Australia's approach to regulating Chinese technologies (Hartcher 2021). At the time, the Government stated it would be prohibiting 'vendors who are likely to be subject to extra judicial directions from a foreign government that conflict with Australian law' (Hartcher 2021). On the advice of the Australian Signals Directorate, it was decided that allowing a Chinese company to provide such fundamental technology infrastructure would be too great a security risk related to large-scale disruptions of critical infrastructure.

The second aspect to be addressed are the considerations for domestic law, which does not present a comprehensive approach to preserving citizen data privacy and security. Over the last 10 years, the development of biometric facial recognition technology, and its capacity to be integrated with CCTV, has amplified the privacy and security

considerations associated with the technology. Since 2015, the Australian Government has been exploring creating a face recognition database using facial photographs from driving licence and passport photos, a database that would effectively become a national facial recognition database. While this has not yet been developed, it remains a likely future prospect. Such a database would operate in association with data from CCTV systems and it highlights that it is possible to identify almost anyone captured in CCTV footage. If a bad actor or foreign state was able to hack a national database, or even a state drivers licence photograph database, data from CCTV footage would be more valuable, assuming it was of sufficient quality, because specific individuals can now be identified more readily (Mann and Smith 2017). The infamous example of the company Clearview AI shows how that might work. The company provides facial recognition software for law enforcement and government agencies and private companies around the world, drawing from billions of images scraped from the internet to identify suspects (Smith and Urbas 2021). Developments such as this demonstrate the growing significance of CCTV systems, as photographic and biometrivnc template datasets, as well as the algorithms used to interrogate them via biometric facial recognition technology, become more sophisticated. This means that there is a greater likelihood that the data captured by CCTV cameras can be used to identify and track individuals, and that this can be applied for a wider range of purposes.

Third, the use of facial recognition in CCTV systems operated by Australian retailers has been widely criticised for their integration of biometric capabilities without the consent—and minimal knowledge—of customers. In 2021, the Office of the Australian Privacy Commissioner found that 7-Eleven breached Australian Privacy Principle 3. It stated that the company's 'large-scale collection of sensitive biometric information through 7-Eleven's customer feedback mechanism was not reasonably necessary for the purpose of understanding and improving customers' in-store experience' (Office of the Australian Information Commissioner 2021).

These examples highlight the expanded use of CCTV to integrate biometric facial recognition and artificial intelligence to multiply the significance of this technology from a regulatory standpoint. The Australian Government and business sector should contemplate that if Chinese cameras do potentially allow the state to access the data, using Chinese companies as intermediaries, this would be a significant national security risk, considering capability developments in facial recognition technology.

In summary, the use of Chinese-made CCTV cameras adds to broader concerns about a lack of regulation of information-collecting technologies, especially as biometric capabilities continue to advance. While it may be possible for governments and corporations to avoid using Chinese-made IoTs in security-sensitive settings, it is not realistic to ban Chinese CCTV cameras or technology in general. Timely and effective regulation of new technologies from the perspective of individual and national interests will be increasingly important.

Conclusion

This paper explained the prevalence of China-made CCTV cameras used in Australia (in particular, the Australian Federal and state governments), articulated the most common national security concerns linked with adopting information-collecting technologies

made in China, and suggested regulatory pathways for Australian state and Federal Government decision-makers. We argue that Australia is likely to remain dependent on China-made information-collecting technologies in at least the medium term because approximately 70 per cent of the world's electronics are made in China (Cheng *et al.* 2019). Therefore, small-scale government bans are not likely to protect Australians' data as Chinese technology companies will be able to continue trade due to the technical sophistication of China-made products and a relative price advantage. National security concerns are, therefore, here to stay, along with those technologies, increasingly pronounced with the prevalence of IoT devices, not only those of Chinese origin.

Among some of the most common concerns are Chinese technology company links with the Chinese Party–state, legal data transfer obligations to China's national and public security agencies, and technical vulnerabilities of IoT CCTV cameras. In the national context of China, the CPC is inseparable from the Government. Additionally, the Party–state offers financial and strategic incentives for private and semi-private actors, such as state subsidies for technology companies expanding overseas, tax breaks, and financial incentives for start-ups. Both Hikvision and Dahua therefore, are bound to the 'authoritarian capitalist dynamic' (Huang and Tsai 2022, 2) and have strong financial incentives to work with the Party–state, like most technology companies establishing themselves domestically in China. In turn, the association with China's domestic market implies a mandate for companies to cooperate with China's national and public security agencies if approached. Refusal to do so may result in warnings, detention, and even criminal responsibility. The market growth of IoT devices increases that risk because devices can transfer data via the internet, making it more vulnerable to hacking and/or backdoor access. As the Australian Government continues to review IoT cybersecurity governance, including critical infrastructure security and security principles for manufacturers (Chalmers 2022), CCTV camera security in the context of their China-based supply chain should also be evaluated.

Due to the lack of strategic trust between Australia and China—in particular, considering the continued large-scale cyberattacks against Australia originating from China—the aforementioned concerns are likely to be considered when evaluating national security risk. In high-risk areas, such as Federal Government buildings, Australian Government agencies are likely to adopt a risk-based approach to adoption of China-made information-collecting technologies. These issues do not require repeated politisation of the national origin of such technologies. Overt politisation of China-made technologies bypasses the urgent concern of IoT under-regulation (Harkin, Mann, and Warren 2022) and the increasing ease of facial recognition technology applications (Mann and Smith 2017). Rather, a targeted technology-specific evaluation of risks approach can be more productively adopted, in addition to known national security concerns.

In both liberal and authoritarian governments, surveillance data is increasingly being used for purposes beyond which it was originally collected. Privacy and identity theft are chief among the concerns raised by lax regulation in this area (Smith and Miller 2022). The issues outlined highlight the fact that a lack of regulation is not only a risk to Australian citizens' privacy and security rights but may also constitute a national security risk for the country.

Australia is unlikely to reduce dependency from China-made CCTV surveillance cameras or other information-collecting digital technologies without a trade

diversification plan. Even if it excludes Chinese-made IoT devices, Australia cannot avoid engaging with them because their dominance in the region ensures unavoidable interaction (Lee 2021). Additionally, similar risks may be presented by other imported technologies or technology parts. A long-term solution should be the broader regulatory regime of emergent information-collecting technologies that would place liability on technology manufacturers to ensure the data privacy and security of their products and services.

Note

1. In this paper, we refer to information-collecting technologies as digital technologies, either software and/or hardware based, that collect or have the potential to collect information.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Ausma Bernot is a Postdoctoral Researcher at the Australian Graduate School of Policing & Security, Charles Sturt University. She has six years of work experience with forensic science and research organisations across the globe, in particular China, where she had the chance to gain insights on how technologies are governed at provincial and national levels.

Her current research focuses on the effects that the merging of infotech and biotech triggers in the fields of governance, surveillance, policing, and public safety. Along with Prof Patrick F Walsh, Dr Ausma Bernot is working to advance the field of Health Security.

Marcus Smith is an Associate Professor in Law. He undertakes research, supervision and teaching in the field of technology law and regulation. His recent publications include *Technology Law: Australian and International Perspectives* (Cambridge University Press, 2021) and *Biometric Identification, Law and Ethics* (Springer, 2021).

ORCID

Ausma Bernot http://orcid.org/0000-0002-2663-1834
Marcus Smith http://orcid.org/0000-0001-9810-979X

References

Amin, A. H. M., N. M. Ahman, and A. M. M. Ali. 2016. Decentralized Face Recognition Scheme for Distributed Video Surveillance in IoT-cloud Infrastructure. Paper presented at the 2016 IEEE Region 10 Symposium (TENSYMP), 9–11 May 2016. https://doi.org/10.1109/TENCONSpring.2016.7519389.

Australian Bureau of Statistics. 2020. "Australia's Trade in Goods with China in 2020." https://www.abs.gov.au/articles/australias-trade-goods-china-2020#cite-window2.

Australian Cyber Security Centre. 2022. "ACSC Annual Cyber Threat Report." https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022.

Australian Government. n.d. "National Security." The Department of the Prime Minister and Cabinet. Accessed August 17, 2023. https://tinyurl.com/49yr3z64.

Australian Research Council. 2020. "Internet of Things Improving Australian Lives." https://www.arc.gov.au/news-publications/media/making-difference-publication/internet-things-improving-australian-lives.
Australian Strategic Policy Institute. n.d.a. "Dahua." Accessed August 17, 2023. https://chinatechmap.aspi.org.au/#/company/dahua.
Australian Strategic Policy Institute. n.d.b. "Mapping China's Tech Giants." Accessed August 17, 2023. https://chinatechmap.aspi.org.au/#/homepage/.
Baker-White, Emily. 2022. "Leaked Audio From 80 Internal TikTok Meetings Shows that US User Data Has Been Repeatedly Accessed from China." *BuzzFeed News*. https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access.
BBC News. 2018. "Huawei and ZTE Handed 5G Network Ban in Australia." https://www.bbc.com/news/technology-45281495.
Bennett Moses, Lyria. 2023. "Australia needs a Robust Cybersecurity Overhaul—not Whack-a-mole Bans on Apps like TikTok." *The Conversation,* April 14. https://theconversation.com/australia-needs-a-robust-cybersecurity-overhaul-not-whack-a-mole-bans-on-apps-like-tiktok-203158.
Bernot, Ausma. 2022. "Transnational State-Corporate Symbiosis of Public Security: China's Exports of Surveillance Technologies." *International Journal for Crime, Justice and Social Democracy* 11 (2): 159–173. https://doi.org/10.5204/ijcjsd.1908.
Boland, Lauren. 2023. "National Cyber Security Centre tells Government departments to avoid TikTok on official devices." *The Journal*, April 21. https://www.thejournal.ie/tiktok-official-devicescyber-security-6049733-Apr2023/.
Bonyhady, Nick, and Matthew Knott. 2023. "TikTok Banned from Government Devices Amid Security Concerns." *Sydney Morning Herald,* April 4. https://www.smh.com.au/politics/federal/federal-government-bans-social-media-app-tiktok-from-public-servants-work-devices-citing-security-concerns-20230404-p5cxxs.html.
Brookes, Joseph. 2022. "Security Agencies Take Advice after Chinese Camera Ban in US, UK." *InnovationAus,* November 30. https://www.innovationaus.com/security-agencies-take-advice-after-chinese-camera-ban-in-us-uk/.
CCTV Calculator. n.d. "CCTV Calculator for Android." Accessed August 17, 2023. https://www.cctvcalculator.net/en/knowledges/vulnerability-database/.
Chalmers, Robert. 2022. "Governing Cybersecurity: Critical Infrastructure, Spies and Consumers." *Law Society of South Australia* 44 (3): 30–31. https://doi.org/10.3316/agispt.20220505066429.
Cheng, Hong, Ruixue Jia, Dandan Li, and Hongbin Li. 2019. "The Rise of Robots in China." *Journal of Economic Perspectives* 33 (2): 71–88. https://doi.org/10.1257/jep.33.2.71.
CyberSecurity Connect. 2021, December 8. "Chinese Cyber Criminals Allegedly Target Australian Power Grid." https://www.cybersecurityconnect.com.au/critical-infrastructure/7408-chinese-cyber-criminals-target-australian-power-grid.
Dahua. "Face Recognition 2.0." Accessed August 17, 2023. https://archive.md/wip/Z8GKa.
Daum, Jeremy. 2017. "Cheatsheet for New Couter-Espionage Rules." *China Law Translate*. https://www.chinalawtranslate.com/en/cheatsheet-for-new-counter-espionage-rules/.
Drinhausen, Katja, and Helena Legarda. 2022. "'Comprehensive National Security' Unleashed: How Xi's Approach Shapes China's Policies at Home and Abroad." *MERICS*. https://www.merics.org/en/report/comprehensive-national-security-unleashed-how-xisapproach-shapes-chinas-policies-home-and.
Dupont, Alan, and William J. Reckmeyer. 2012. "Australia's National Security Priorities: Addressing Strategic Risk in a Globalised World." *Australian Journal of International Affairs* 66 (1): 34–51. https://doi.org/10.1080/10357718.2011.637316.
Federal Communications Commission. 2022. "FCC Bans Authorizations for Devices That Pose National Security Threat". https://www.fcc.gov/document/fcc-bans-authorizations-devices-pose-national-security-threat.
Ferguson, Victor, and Darren J. Lim. 2021. "Economic Power and Vulnerability in Sino-Australian Relations." In *China Story Yearbook: Crisis*. Canberra: ANU Press. https://doi.org/10.22459/CSY.2021.09.

Fu, Jingying, and Hua Qin. 2021. "The Information Office of the Ministry of State Security answers the reporter's questions [国家安全部新闻办答记者问]." *People's Daily,* January 8. https://archive.md/bSw9p.

Gao, Kathy. 2019. "Where Next For China's Technology Policy? Creating the Industrial Internet." *BloombergNEF,* December 9. https://about.bnef.com/blog/where-next-forchinas-technology-policy-creating-the-industrial-internet/.

Gavrovska, Ana, and Andreja Samčović. 2020. "Intelligent Automation Using Machine and Deep Learning in Cybersecurity of Industrial IoT: CCTV Security and DDoS Attack Detection." In *Cyber Security of Industrial Control Systems in the Future Internet Environment*, edited by Ana Gavrovska, and Andreja Samčović, 19. https://doi.org/10.4018/978-1-7998-2910-2.ch008.

Geiger, Chas, and Zoe Kleinman. 2023. "TikTok: UK Ministers Banned from Uning Chinese-Owned App on Government Phones." *BBC News,* March 18. https://www.bbc.com/news/uk-politics-64975672.

Golley, Jane, Amanda Barry, Paul Harris, and Darren J. Lim. 2020. "Geoeconomics and the Australian University Sector: A 'geoeducation' Analysis." *Security Challenges* 16 (4): 24–40. https://www.jstor.org/stable/10.230726976256.

Harkin, Diarmaid, Monique Mann, and Ian Warren. 2022. "Consumer IoT and its Under-Regulation: Findings from an Australian Study." *Review of. Policy & Internet* 14 (1): 96–113. https://doi.org/10.1002/poi3.285.

Hartcher, Peter. 2021. "Huawei? No Way! Why Australia Banned the World's Biggest Telecoms Firm." *The Sydney Morning Herald*. https://www.smh.com.au/national/huawei-no-way-why-australia-banned-the-world-s-biggest-telecoms-firm-20210503-p57oc9.html.

Hawes, C. 2022. *The Chinese Corporate Ecosystem*. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781108937276.

Hikvision. n.d. "7-inch 4 MP 32X Powered by DarkFighter IR Network Speed Dome." Accessed August 17, 2023. https://archive.md/wip/hJr8k.

Huang, Jingyang, and Kellee S. Tsai. 2022. "Securing Authoritarian Capitalism in the Digital Age: The Political Economy of Surveillance in China." *Review of. The China Journal* 88: 2–28. https://doi.org/10.1086/720144.

Huawei. n.d. "Does China's National Intelligence Law Compel Huawei to Plant so-called "Backdoors" in Telecommunications Infrastructure?" Accessed August 17, 2023. https://archive.md/FZ7yy.

Hussain, M. 2021. "CPEC and Geo-Security Behind Geo-Economics: China's Master Stroke to Counter Terrorism and Energy Security Dilemma." *East Asia* 38 (4): 313–332. https://doi.org/10.1007/s12140-021-09364-z.

IDC. 2021, April 22. "China's Public Cloud Service Market Leads the World in Growth." https://web.archive.org/web/20230105035702/.

Jiang, Jue. 2021. "The Eyes and Ears of the Authoritarian Regime: Mass Reporting in China." *Journal of Contemporary Asia* 51 (5): 828–847. https://doi.org/10.1080/00472336.2020.1813790.

Laurenceson, James. 2018. "Do the Claims Stack Up? Australia Talks China." Australia-China Relations Institute. https://www.australiachinarelations.org/content/do-claims-stack-australia-talks-china.

Lee, John. 2021. "China, Australia, and the Internet of Things." *The Interpreter,* December 17. https://www.lowyinstitute.org/the-interpreter/china-australia-internet-things.

Mann, Monique, and Marcus Smith. 2017. "Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight." Review of." *The University of New South Wales Law Journal* 40 (1): 121–145. https://search.informit.org/doi/pdf/10.3316ielapa.771179858194317.

Mason, Max. 2022. "TikTok Australia Revenue Surges as Facebook Rivalry Heats Up." *Financial Review*, August 8. https://www.afr.com/companies/media-and-marketing/tiktok-australia-revenue-surges-as-facebook-rivalry-heats-up-20220802-p5b6oa.

McGeachy, Hilary. 2022. "The Changing Strategic Significance of Submarine Cables: Old Technology, new Concerns." *Review of. Australian Journal of International Affairs* 76 (2): 161–177. https://doi.org/10.1080/10357718.2022.2051427.

Migliano, Simon, and Samuel Woodhams. 2021. "Hikvision and Dahua Surveillance Cameras: Global Locations Report." In *Top10VPN*. https://www.top10vpn.com/research/hikvision-dahua-surveillance-cameras-global-locations/.
Miller, Charles. 2022. "Explaining China's Strategy of Implicit Economic Coercion. Best Left Unsaid?" *Review of. Australian Journal of International Affairs* 76 (5): 507–521. https://doi.org/10.1080/10357718.2022.2061418.
Ministry of Foreign Affairs of the PRC. 2023. "Foreign Ministry Spokesperson Mao Ning's Regular Press Conference on February 9, 2023." https://archive.md/BaHnl.
Mizen, Ronald. 2022. "Imports from China hit Record $10.6b in August." *Financial Review,* October 6. https://tinyurl.com/bdd3643x.
Needham, Kirsty, and Clare Baldwin. 2021. "China's Gene Giant Harvests Data from Millions of Women." *Reuters,* July 7. https://tinyurl.com/2p8f5am5.
Office of the Australian Information Commissioner. 2021, October 14. "OAIC Finds against 7-Eleven over Facial Recognition." https://tinyurl.com/mtnkbc39.
Paganini, Pierluigi. 2022. "Over 80,000 Hikvision Cameras can be Easily Hacked." *Security Affairs,* August 23. https://securityaffairs.co/134756/security/hikvision-cameras-vulnerability.html.
Paleri, Prabhakaran. 2008. "National Security: Imperatives and Challenges." Tata McGraw-Hill.
Paterson, James. 2023. "Audit: Commonwealth Riddled by CCP Spyware." In *Senator James Paterson's page*. https://james-paterson.webflow.io/news/media-release-audit-commonwealth-riddled-by-ccp-spyware.
Pearson, Margaret M., Meg Rithmire, and Kellee S. Tsai. 2022. "China's Party–State Capitalism and International Backlash: From Interdependence to Insecurity." *International Security* 47 (2): 135–176. https://doi.org/10.1162/isec_a_00447.
PwC. 2018. "Australia's IoT Opportunity: Driving Future Growth." https://www.pwc.com.au/publications/australias-iot-opportunity.html.
Rickards, James G. 2009. "Economic Security and National Security: Interaction and Synthesis." *Strategic Studies Quarterly* 3 (3): 8–49. http://www.jstor.org/stable/26268663.
Roberts, Anthea, and Nicolas Lamp. 2021. *Six Faces of Globalization*. Cambridge, MA: Harvard University Press. https://doi.org/10.4159/9780674269811.
Saunokonoko, Mark. 2021. "Australia Prepares for China Retaliation after Blaming Beijing for Microsoft Hack." *The Sydney Morning Herald*, July 20. https://www.smh.com.au/world/australia-prepares-for-china-retaliation-after-blaming-beijing-for-microsoft-hack-20210720-p58bbe.html.
Schaefer, David. 2018. "Australia's new Alliance Dynamics, US–China Rivalry and Conflict Entrapment in Outer Space." *Australian Journal of International Affairs* 72 (1): 31–48. https://doi.org/10.1080/10357718.2017.1337714.
Shepardson, David. 2023. "White House Sets Deadline for Purging TikTok from Federal Devices." *Reuters,* February 28. https://www.reuters.com/technology/white-house-gives-agencies-30-days-impose-federal-device-tiktok-ban-2023-02-27/.
Simon, Tobby. 2017. "Critical Infrastructure and the Internet of Things" in "Global Commission on Internet Governance: Cyber Security in a Volatile World." *The Centre for International Governance Innovation and the Royal Institute of International Affairs*. https://www.cigionline.org/publications/critical-infrastructure-and-internet-things-0/.
Smith, Marcus, and Seumas Miller. 2022. "The Ethical Application of Biometric Facial Recognition Technology." Review of." *AI & Society* 37 (1): 167–175. https://doi.org/10.1007/s00146-021-01199-9.
Smith, Marcus, and Gregor Urbas. 2021. *Technology law: Australian and International Perspectives*. Cambridge: Cambridge University Press.
The Standing Committee of the PRC. 2017. "PRC National Intelligence Law (as amended in 2018) [中华人民共和国国家情报法（2018年修正本）]." In *Smart Law Popularisation Platform*. https://archive.md/wip/tGEI0.
The State Council of the PRC. 2015, May 19. "'Made in China 2025' Plan Issued." https://archive.md/wHBjm.

TikTok. n.d. "About Project Texas." Accessed August 17, 2023. https://archive.md/80gsD.
Trevaskes, S., and A. Bernot. 2023. "Surveillance Infrastructure in China: Key Concepts and Mechanisms Enhancing the Party–State's Governance Ambitions." *Global Media and China* Online First. https://doi.org/10.1177/20594364231171013.
U.S.–China Economic and Security Review Commission. 2018. "2018 Annual Report to Congress." https://www.uscc.gov/annual-report/2018-annual-report-congress.
Vinall, Marnie. 2023. "TikTok to be banned from state government devices following federal move." *The Sydney Morning Herald,* April 3. https://www.smh.com.au/politics/federal/tiktok-to-be-banned-from-state-government-devices-following-federal-move-20230403-p5cxsz.html.
Xiao, Jinbo, Jinying Fu, and Jinjin Su. 2021. "Acts that Endanger National Security may be Around Us [危害国家安全行为 可能就在我们身边]." *People's Daily*. https://archive.md/lEz9b#selection-1059.0-1059.17.
Xu, Xiaofei, Eve Brennan, and James Frater. 2023. "EU Bans TikTok for Official Devices across All Three Government Institutions." *CNN News,* March 1. https://tinyurl.com/5d7ncc4p.