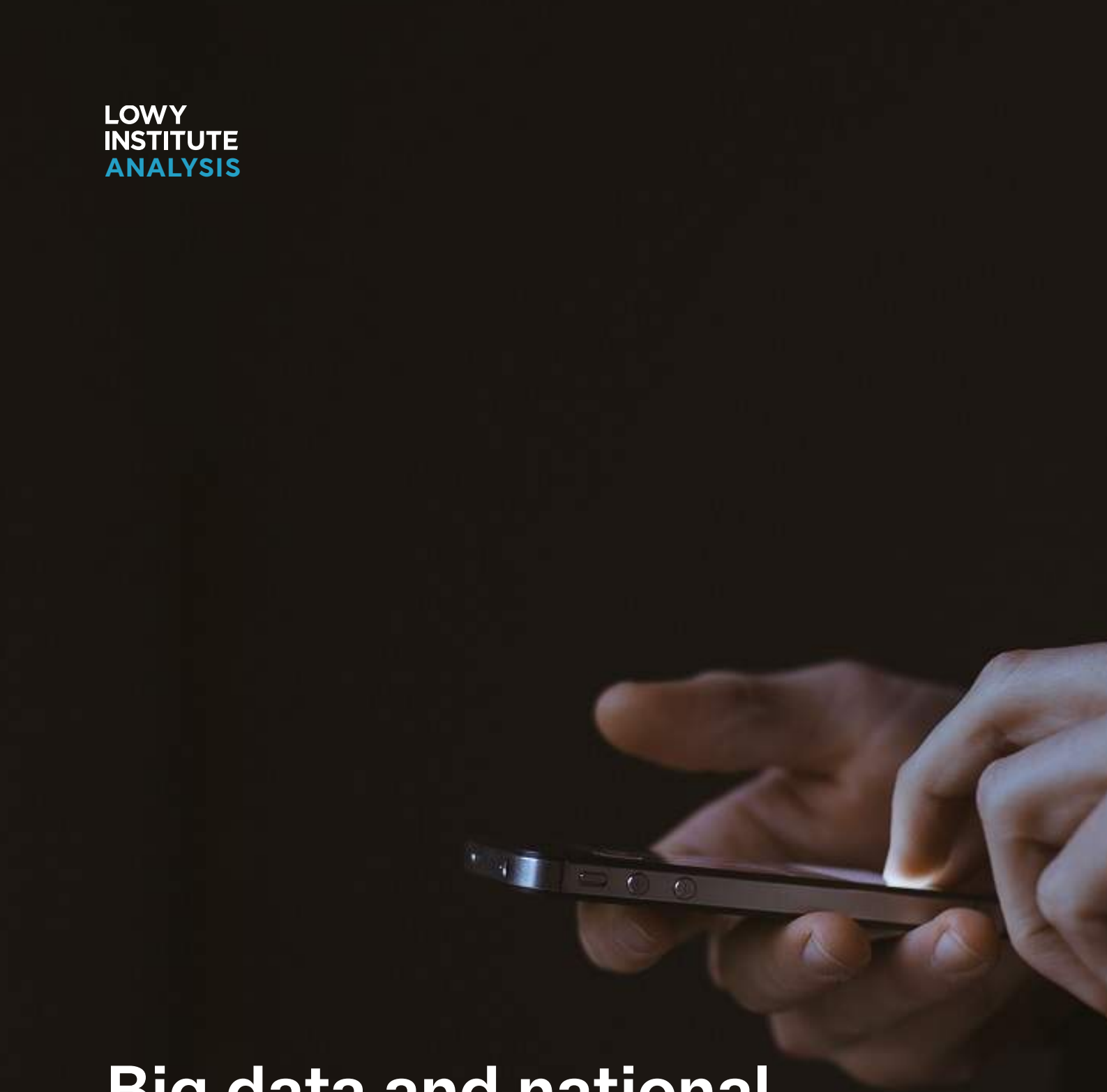
LOWY INSTITUTE ANALYSIS



Big data and national security: A guide for Australian policymakers

MIAH HAMMOND-ERREY

FEBRUARY 2022

The Lowy Institute is an independent policy think tank. Its mandate ranges across all the dimensions of international policy debate in Australia — economic, political and strategic — and it is not limited to a particular geographic region. Its two core tasks are to:

- produce distinctive research and fresh policy options for Australia's international policy and to contribute to the wider international debate

- promote discussion of Australia's role in the world by providing an accessible and high-quality forum for discussion of Australian international relations through debates, seminars, lectures, dialogues and conferences.

Lowy Institute Analyses are short papers analysing recent international trends and events and their policy implications.

The views expressed in this paper are entirely the authors' own and not those of the Lowy Institute.

KEY FINDINGS

- Data abundance, digital connectivity, and ubiquitous technology now enable near complete coverage of human lives across the planet, often in real-time. The Covid-19 pandemic, by forcing more interactions online and greater social reliance on technology, has significantly added to the global pool of data.

- Advances in the scale, application, and commercial uses of data significantly outpace regulation of the big data landscape. Technical and analytical capabilities that are essential for the functioning of societies are increasingly concentrated in the hands of a small number of commercial entities.

- The implications of big data for surveillance, real or potential interference, and kinetic war are underappreciated in policy and public discussions. Identifying and protecting the uses of critical data should be a national security priority for government on par with safeguarding critical digital infrastructure.

EXECUTIVE SUMMARY

Big data has created a complex new information and infrastructure landscape. Big tech companies that have capitalised on its three core features — data abundance, digital connectivity, and ubiquitous technology — are the new oligarchies and are increasingly controlling the capabilities essential for a functioning society.

Big data has profound impacts on society. It enables everything from access to knowledge and global communication, to delivery of services and infrastructure. However, big data is exacerbating existing national security threats and creating new and unpredictable ones. It can be weaponised for war, providing information dominance and kinetic targeting capability. Big data has the capacity to enable or eliminate the barriers of entry for surveillance and oppression. It drives information warfare as well as social and political interference.

An understanding of the potential harms from the misuse of big data and big tech is beginning to emerge, but much of its impact remains obscure. It is important for Australia to understand and counter the threats enabled by big data at a critical time for regional security.

INTRODUCTION

The reach, impact, volume, and speed of data has changed the way states, businesses, groups, and individuals communicate and make sense of the world.[1] Data is remodelling society's relationship with government, changing participation in the economy and access to services, as well as challenging trust in social, commercial, and government institutions.[2] Big data is also redefining national security[3] and the way nations protect individual rights and freedoms.[4]

Big data is loosely defined as data that is too large to be manually processed. It allows literally millions of pieces of information — from location points, financial transactions, and social media profiles, to medical files and video streams — to be brought together and analysed. The analytics and technologies used to derive value and insight from this data,[5] such as artificial intelligence (AI) and machine learning (ML), should be considered part of big data.

This paper is in two sections. The first outlines the foundations of the big data landscape. It examines how the ubiquity of technology — our daily reliance on data infrastructure and our participation in the landscape — forms the backbone of the new economic, political, and social power of institutions. The second section outlines how big data technologies are adding new threats to national security[6] and exacerbating existing ones. This comes at a time when Australia's strategic circumstances are more malign than in recent decades.[7] In this environment, Australia needs to leverage big data and emerging technologies for strategic advantage.

THE BIG DATA LANDSCAPE

Big data and emerging technologies have transformed the global information landscape and national security operating environment. Big data transfers power to organisations that hold the most data, control global data and information flows, and provide digital connectivity. It creates oligarchies among companies whose technology is the most ubiquitous.

These powerful private entities have created a new information and infrastructure landscape with minimal oversight from national governments. In this environment, technical developments occur much faster than regulation. The pace of development, combined with the complexity and interdependence of technologies, along with issues of global reach complicate the work of legislators and regulators, who are largely not digital natives.

As people go about their daily lives, their activity creates digital footprints, making it virtually impossible to exist without leaving a digital trace. Google's trackers are present on more than 80 per cent of 1000 popular websites in Australia *(Stock Catalog/Flickr)*

Big data arose from technical advances in storage capacity, processing speed, and the declining cost of data collection and analysis as well as the move towards understanding data as continuously collected, almost infinitely networkable, and highly flexible.[8]

Big data "is less about data that is big than it is about a capacity to search, aggregate, and cross-reference large data sets"[9] to analyse and

derive insight,[10] usually to create economic value.[11] Previously, databases were unable to simultaneously deal with what are known as the 3Vs of big data: volume, velocity, and variety.[12] But increased computational power, new database designs, and distributed storage now enable collection and analysis of big data.[13] The definition has subsequently been expanded to 5V to include veracity (determining uncertainty and inconsistency in data) and value (gaining insights into and from data).[14]

There are three features of big data with unique and significant implications for national security: data abundance, digital connectivity, and ubiquitous technology.[15] (See Figure 1). These features create a big data landscape that concentrates the data, technical capabilities, and analytical capacity that are increasingly essential for functioning societies.

Figure 1:
Features of big data

1. Data abundance

"Data abundance" refers to the vast and rapidly growing volume of digital information that exists in society.[16] By 2020, the number of bytes (units of memory size) in the digital universe was 40 times the number of stars in the observable universe.[17] There are three primary locations where digital content is created: the core (traditional and cloud data centres), the edge (enterprise-hardened infrastructure, such as cell towers and branch offices), and the endpoints (personal computers, smart phones, and Internet of Things (IoT) devices). The summation of all the data collected in these locations, whether it is created, captured, or replicated, is sometimes called the global datasphere.[18]

Case Study 1 | What kinds of data do companies collect?

Australian airline Qantas collects data about their 13 million frequent flyer members and millions of other consumers who use their services.[19] This includes, but is not limited to, travel details and identity documentation, biometric data (CCTV, facial recognition in airports, and passport photographs), contact and address details, payment and financial information, health and dietary information, geolocation, IP addresses of devices, employer details, shareholder names, tax file numbers, and bank account details.

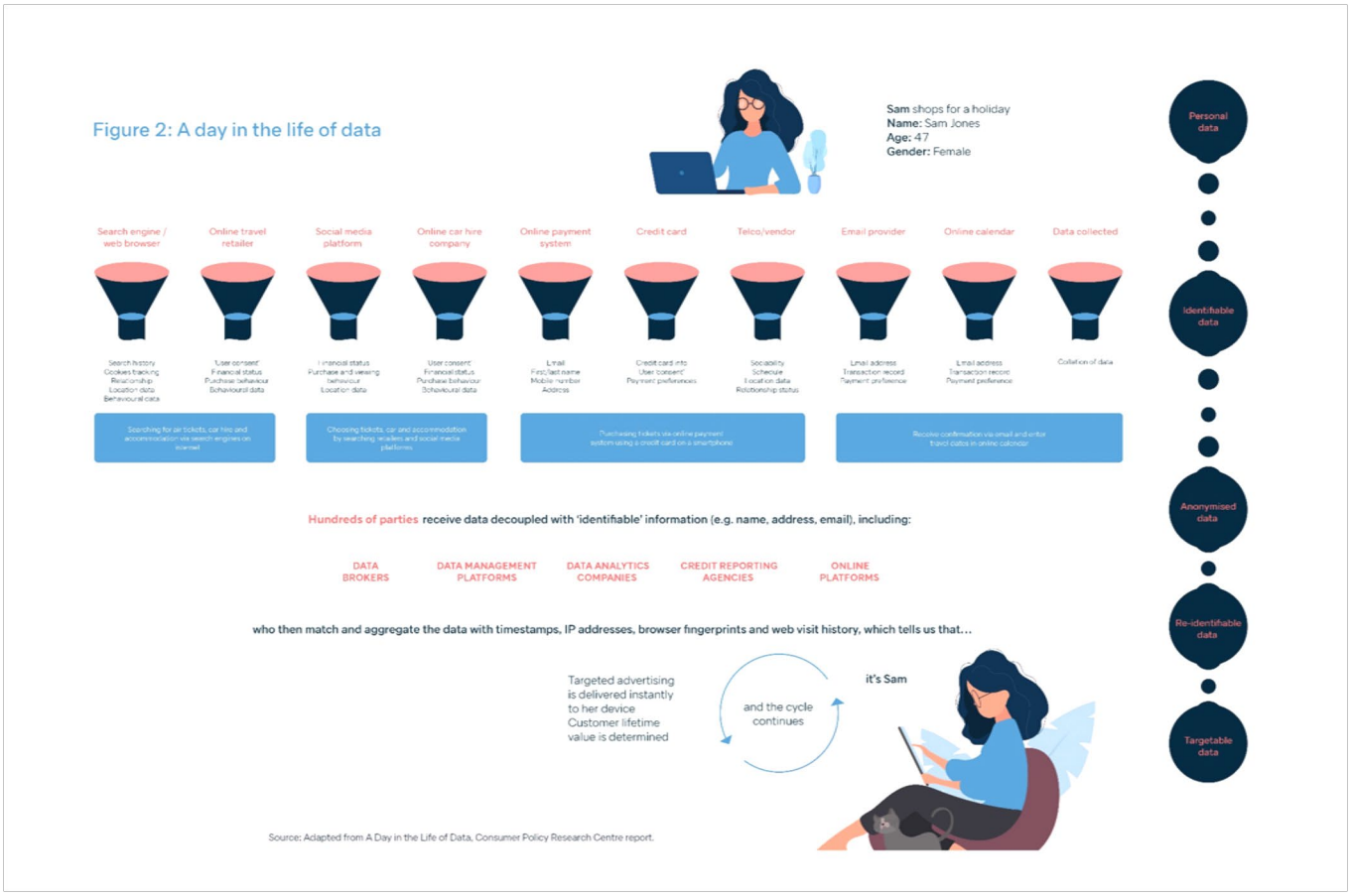
The Qantas privacy policy[20] notes that the company may collect and handle sensitive personal information, such as health, racial or ethnic origin, political opinions, religious beliefs, trade union membership, or sexual orientation. The list of information Qantas indirectly collects includes social media details and third-party data from a wide range of partners and service providers. The amount of data held about individuals by private entities is extremely difficult to quantify, but Qantas is not unusual or particularly large by global corporate standards.

The *amount* of data is not the whole story. The ability to represent the interactions of daily social life in online, quantified data — datafication — has increased dramatically.[21] While datafication is not entirely new, it is increasingly sophisticated and nuanced. Big data has made data

collection about human interactions — including aspects that were previously unrecorded — omnipresent. As people go about their daily lives, their activity leaves digital footprints,[22] with data constantly created by their movements and activities,[23] making it virtually impossible to exist without leaving a digital trace.[24]

Much of this increase in datafication has been driven by the development and adoption of smart phone technology. On average, global users interact with their mobile phones hundreds of times per day. The average Australian spends 5.5 hours per day on their phone.[25] Much of this data is generated through the daily habits of social media, shopping, searching online, and fitness tracking, but large volumes of data are also created and collected by machines to track the daily lives of users.[26] (See Case Study 1).

This abundance of data (and sometimes the absence of it) enables those who collect it to make inferences about the beliefs, values, preferences, psychological state, and intimate details of those who produce it, including people's feelings and vulnerabilities.[27] These inferences are made about individuals, often without their knowledge, by the aggregation of data collected from seemingly mundane activities. In short, big data has exploded the scope of personal and personally identifiable information.[28] Some data is individualised and some of it is collected in so-called "anonymised" data sets, although almost all of it can be re-identified to the individual level.[29] It is possible to build an increasingly comprehensive picture about people and things from data alone, even if that data is anonymised, as illustrated in Figure 2.



Datafication is an inherently commercial activity. Most data is created by and resides in the private sector, in tech companies, and with data brokers, as does the analytical capability to make sense of it. Data broking companies aggregate personally identifiable information about consumers from different sources, then match, license, and sell that information.[30] Commercial data sets are created, bought, and sold by third party data brokers, acquired by purchase from private companies and by trawling public information sources.[31]This constitutes the big data economy and the commercial value of data is linked to whether it can be attributed to an individual's identity — the more data obtained, the more granular a profile it produces.[32] The deeper the level of detail, the more targeted individual advertising can be. Large commercial data sets can be purchased by anyone, including in some countries by state security services and government organisations.

To provide a sense of the size of this market, of the 4000 data brokers globally, one of the largest, Acxiom, is said to have 3000 data points per person for 500 million consumers worldwide.[33] The global data broker industry was estimated to be worth US$178 billion in revenue in

The number of devices connected to the internet has increased exponentially over the past 20 years. Estimates vary between 100 and 200 billion devices connected at the end of 2020.

2018, and PricewaterhouseCoopers market researchers suggest that by 2025, the global data economy will be worth more than US$400 billion.[34] Estimates suggest that Google, Amazon, Microsoft, and Facebook alone store at least 1200 petabytes, or 1.2 million terabytes, of data between them.[35] However, the true size of the market is unknown, as brokers operate with little or no transparency in primarily unregulated spaces.[36] Large data stores held by commercial actors are vulnerable to hacking and exploitation by nation states and criminal actors,[37] as seen by the breaches at Equifax, a multinational consumer credit reporting agency, in 2017; the Australian National University in 2018; and data collection company Oxydata in 2019.[38]

2. Digital connectivity

Digital connectivity is the ability to connect people, places, and ideas through virtual networks.[39] Digital connectivity includes billions of sensors and devices around the world connected to the internet.[40] It includes the relationship between things and people made possible by networked technologies and various platforms,[41] such as computers, mobile phones, and the Internet of Things (IoT), enabling previously unconnected agents to connect.[42]

The number of devices connected to the internet has increased exponentially over the past 20 years. Estimates vary between 100 and 200 billion devices connected at the end of 2020.[43] When individuals use devices to send, receive, broadcast, and share information, digital connectivity is most visible.[44] Less visible is the vast network of billions of sensors in sectors such as business, manufacturing, healthcare, retail, security, public places, transportation, and in "smart" home devices.[45] In 2020, machine-to-machine communications accounted for 40 per cent of the total traffic between sensors and this ratio will continue to rise. Unprecedented digital connectivity makes it very difficult for people and objects to move through space without detection — a profound change in the past two decades for citizens and national security agencies.

3. Ubiquitous technology

Ubiquitous technology is the pervasiveness of technology in individuals' lives and extent to which they interact with it, knowingly or unknowingly. Phones and computers are so deeply embedded in human lives[46] that it is easy to forget that much of the technology is barely older than teenagers. Google started in 1998. Facebook is 17,

YouTube is 16, and the iPhone is merely 15 years old. The way the world produces, handles, and sells data has changed so much in such a short time that regulation, access, and understanding have struggled to keep pace.

Contactless payment, which has become almost ubiquitous in the last two years due to Covid-19 restrictions, is an integral part of big data collection
(Jonas Leupe/Unsplash)

Other technologies are equally ubiquitous but less visible, such as the analytics that make sense of data, and the sensors that are omnipresent in the environment. The processes and practices of AI are also pervasive and driven by big data — although often the technical sophistication is pseudo-scientific and makes unsubstantiated claims and assumptions about human behaviour.[47] Big data underpins the future of AI, a term that has become more prominent in the past 10 years and which is often used as a marketing phrase, diluting its meaning and importance.

Australian technologist and engineer Genevieve Bell says it is important to think about AI not as an individual technology, but as a "constellation of technologies…You will not get to AI without data, but whatever that data is will shape AI profoundly and absolutely".[48] Her key message is that individuals are not always aware that their daily interactions are fuelling technological innovation outside their view.

CONCENTRATION OF TECHNICAL CAPABILITIES

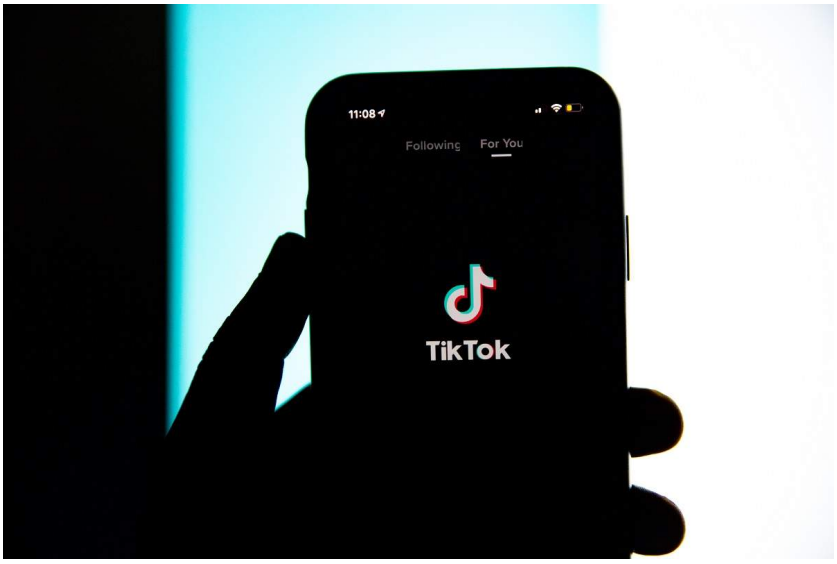
According to the former head of the UK's intelligence and security organisation, these tech companies have "come to know much more about us and our personal habits and tastes than any intelligence agency ever could (or should)".

The technology sector has become increasingly dominated by a small number of companies, which concentrates information flows, critical data sets, and the technical capabilities essential for functioning democracies. A handful of companies have monopolised areas of data abundance, digital connectivity, and ubiquitous technology, creating an "infrastructural core" or ecosystem upon which most other applications and platforms are built.[49] They are therefore able to control global data flows and information services[50] in an unprecedented way. Historical monopolies such as the East India Company, the Vanderbilt empire, Rockefeller's Standard Oil, and Carnegie Steel wielded similar power. However, contemporary commercial power resides in and through data and information, in addition to its economic weight. This represents a new power base for private enterprise.

Alphabet (Google), Apple, Facebook, Amazon, and Microsoft dominate their market sectors, with unprecedented data stores and analytical capabilities conferring market power.[51] Virtually everyone else — government agencies included — depend on these big tech companies at some level for their infrastructure and information services, particularly cloud computing infrastructure.[52] China has a similar set of firms in Alibaba, Baidu, and Tencent, which are less widely used in the West, [53] although the global appeal of video sharing service TikTok, owned by Chinese company ByteDance, and the regional appeal of instant messaging service WeChat and others may be a sign of things to come. According to the former head of the UK's intelligence and security organisation, these tech companies have "come to know much more about us and our personal habits and tastes than any intelligence agency ever could (or should)".[54]

Companies that have monopolised data abundance, digital connectivity, and ubiquitous technology largely control global data flows and analytics, information services, and risks. Since virtually all information is now controlled by or goes through these large technology companies, the security landscape for government has fundamentally changed, creating unprecedented interconnectivity and vulnerability.[55] The Covid-19 pandemic has further accelerated digitalisation in society and contributed to widening power asymmetries between consumers and big tech companies.[56]

While government regulation globally tries to catch up, big tech companies have amassed immense power. In Australia, regulation tends to focus on specific aspects of data abundance, digital connectivity, and ubiquitous technology rather than on the overall landscape. For example, the Australian Competition and Consumer Commission's Digital Advertising Services Inquiry into anti-competitive behaviour[57] is part of a five-year Digital Platform Services Inquiry (2020–2025), while its News Media Bargaining Code[58] focuses on content distribution.



The phenomenal appeal of global video sharing service TikTok, owned by Chinese company ByteDance, gives the firm unprecedented data stores and analytical capabilities *(Solen Feyissa/Flickr)*

The top five big tech American firms have a market value of approximately US$9.5 trillion and earned revenues of around US$1.2 trillion last year.[59] Combined, their market capitalisation is more than five times Australia's gross domestic product, while their annual earnings are more than twice Australia's federal government fiscal revenue for 2020.[60] Big data is essential for continued success in the technology market and increasingly across all sectors of society, including the delivery of government services. Big tech's data dominance is a potent barrier to market entry for others, endowing substantial market power to the largest platforms.[61] This has given the companies control over global data stores, information flows, and services. Consequently, they wield enormous economic and infrastructural power.

Identifying and protecting data on citizens may be just as important as protecting other critical infrastructure. Yet big data has shifted the parameters of who creates and owns information about Australians, and who owns and operates the infrastructure many of our services rely on. The big data landscape is enabling new, non-state actors, primarily tech companies, to deny or change citizen access to services in a way that is at times inconsistent with democratic values and anti-discrimination laws, and which is largely unregulated. For example, algorithmically-driven systems can offer, deny, or mediate access to services or opportunities to people differently, and perpetuate over-monitoring and over-policing of minority groups.[62] Lack of algorithmic, data, and company transparency makes it difficult to fully comprehend and quantify the nature of the threat.

BIG DATA AND AUSTRALIA'S STRATEGIC ENVIRONMENT: THREE EMERGING THREATS

The big data landscape shapes many of the contemporary security challenges Australia faces. Three emerging threats to national security and nation-state power emerge from the big data landscape. First, big data can confer a strategic advantage by enabling information dominance and improving kinetic targeting capability — the application of active military force. Second, big data enables and "democratises" targeting and surveillance. Third, big data drives information warfare as well as social and political interference.

These threats are emerging in the context of a security environment that the Australian government's 2020 Defence Strategic Update describes as "markedly different from the relatively more benign one of the past".[63] Confidence in the rules-based global order is being undermined by disruptions from a widening range of sources. Expanding cyber capabilities — and the willingness of some countries and non-state actors to use them — are complicating the strategic environment. Major power competition has intensified and the prospect of high-intensity conflict in the Indo-Pacific, while still unlikely, is less remote. The prevalence of grey zone activities has increased in the Indo-Pacific, involving military and non-military forms of assertiveness and coercion, including rogue cyberattacks targeting Australia's data infrastructure. The actions are aimed at achieving strategic goals without provoking broad-scale conflict. Such activities have ranged from militarisation of the South China Sea and active interference to big data-enabled information operations, disinformation campaigns, and economic coercion.[64]

Covid-19 has accelerated the use of digital technologies and pushed more interactions online, significantly adding to the global pool of data and increasing social dependence on technology.

Covid-19 has accelerated the use of digital technologies and pushed more interactions online, significantly adding to the global pool of data[65] and increasing social dependence on technology. Online interactions encourage "echo chambers", which can polarise society, promote distrust, and create more opportunities for malign interference.[66]

Domestically, Australia faces evolving threats, too. The 2020 Annual Report from the Australian Security Intelligence Organisation (ASIO) notes that the terrorism threat level remains at "probable", with no prospect it will be lowered in the foreseeable future.[67] Religiously

motivated violent extremism remains a significant and real concern.[68] Ideological extremism is more organised, sophisticated, and active.[69] Big data is a force multiplier for all forms of extremism.[70]

Espionage and foreign interference also represent threats to Australia's way of life. There are more foreign spies and their proxies operating in Australia than there were at the height of the Cold War.[71] Foreign governments are seeking information about Australia's capabilities, research and technology, and domestic and foreign policy.[72] The big data landscape is changing modern spy craft and expanding the avenues for intelligence collection, as well as offering new ways to identify adversary intelligence operations.[73] The big data landscape expands the techniques available to adversaries to obtain this information and makes them harder to identify and disrupt.[74]

In addition to traditional ways to inflict damage on an organisation, the big data landscape adds potential new vectors, such as altered or corrupted data *(Markus Spiske/Unsplash)*

Recognition of the role cybersecurity plays in national security is now much more broadly understood, with a growing raft of measures to address it. However, other aspects of the big data landscape, such as identifying and protecting vulnerable and critical data sets, remain largely unaddressed. The big data landscape is challenging existing models of harms assessment, which have historically been focused on direct physical harm and economic harm.

There are now myriad ways to attack an organisation or individual, with some traditional methods still available only to nation states, but many

more available to a wider range of entities. For example, a stock exchange could be impacted in traditional ways by malicious actors, such as through physical damage or destruction, cyberattack, or natural or human-instigated disasters such as flooding or power failure. The big data landscape adds potential new vectors, such as altered or corrupted data, coordinated price manipulation on a mass scale, or information operations resulting in real or perceived insider trading that generates fear in the institutions' ability to function or lack of trust in its integrity.

The military utility of sensing and communications functions and the enhanced potential it offers to target adversaries in conflict is of critical concern.

1. Big data confers strategic advantage: information dominance is military dominance

Big data can dramatically improve situational awareness and can be weaponised in war to target adversaries. When well integrated into command-and-control systems, information dominance produces military dominance[75] and big data offers global situational awareness on a scale previously not possible. If analysed and processed effectively, big data can be used to outpace an adversary's decision-making processes. It also offers the ability to challenge or deny an adversary's situational awareness by poisoning data sets and running adversarial AI systems. It can be used in war to improve targeting for kinetic action.

Big data produced by remote sensors on a large scale can confer strategic advantage by providing situational awareness. It can be integrated into space-based systems and targeting systems to help gain control of territory and territorial approaches, deter traditional military activities, and create uncertainty about the safety of transit in disputed territories. For example, China has deployed a network of remote sensors and communications capabilities in the South China Sea between Hainan Island and the Paracel Islands.[76] Big data capabilities are part of the Blue Ocean Information Network developed by China Electronics Technology Group Corporation (CETC), a state-owned defence company[77] on the US Entity List.[78] Plans for the Blue Ocean Information Network involve expanding the sensor and communications network to the rest of the South China Sea, the East China Sea, and other ocean areas far from Chinese territory.[79]

The military utility of sensing and communications functions and the enhanced potential it offers to target adversaries in conflict is of critical concern. Remote sensors and big data analytics are being combined with traditional Intelligence, Surveillance, and Reconnaissance (ISR)

The ability to produce a more complete picture of society and individual behaviour creates the potential for a society that is more invasive and repressive of individual autonomy.

platforms using AI applications as part of the Chinese People's Liberation Army (PLA) approach to "intelligentised warfare".[80] The ability to triangulate exact locations based on an array of sensors, especially many that are much cheaper than traditional ISR assets, has particular significance for military transit. As one military commentator noted in relation to military technologies and systems on Chinese-claimed island reefs in the Spratly Islands, "the combined information power capabilities on China's SCS [South China Sea] outposts…will work synergistically prior to and throughout the military operations to preserve the PLA's access to information in the SCS battlespace while simultaneously denying an adversary access to information."[81] In conjunction with traditional military assets, these capabilities provide China with the infrastructure to control large areas, even in international waters.[82]

2. Big data enables targeting, surveillance, and oppression

Big data enables the targeting and surveillance of humans, often in real time. It enables invasive identification of and sometimes complete access to physical and online activity, locations, and movement. The scope for causing individual and societal harm is significant. The volume of personal or personally identifying information available and degree of datafication and connectivity means comprehensive profiles of individuals, interest groups, institutions, political groups, and nation states can be quickly and remotely created. From an individual perspective, this is often expressed as a concern about privacy intrusion, however, from a national security perspective, the big data landscape offers new potential for surveillance and targeting.

The ability to produce a more complete picture of society and individual behaviour creates the potential for a society that is more invasive and repressive of individual autonomy.[83] In the near future, it will become almost impossible to escape digital surveillance[84] — Google's trackers are present on more than 80 per cent of 1000 popular websites in Australia.[85] The national security implications of near complete data coverage of human lives — which enables tracking, monitoring, and analysis, sometimes in real-time[86] — are underappreciated in policy and public commentary.

An example is the extensive and well-documented surveillance and detainment of Uighurs in Xinjiang, which is enabled by a combination of big data collection and data fusion, among other forms of

surveillance.[87] Another example is the high-end spyware Pegasus, designed by Israeli cyber arms firm NSO Group to track terrorists and criminals. It was recently revealed that despite Israeli export controls, Pegasus has been used to spy on journalists, human rights activists, government ministers, diplomats, and businesspeople in democracies and autocratic regimes.[88]

The surveillance of myriad human actions and interactions, often in real time, has significant national security implications, which are often underappreciated in policy and public commentary
(Bernard Hermant/Unsplash)

Big data "democratises" the capabilities underpinning targeting and surveillance — functions previously reserved for nation states and their governments. The big data digital footprint and infrastructure used to analyse it is predominately owned by commercial entities, meaning that the data — and ability to derive insight from it — largely resides in the private sector. Much of this collection occurs within companies that monetise their user data and much of it is available for purchase.[89] The scale of data, often accessible in real time, creates uncertainty over when, where, and by whom aggregation, targeting, and surveillance can occur. Where once states exercised surveillance with external authorisation and oversight, big data systems enable tracking, monitoring, and analysis, and make these capabilities accessible to many more actors, in opaque environments with varying, sometimes non-existent, degrees of regulation of their activities.

The pre-conditions already exist for adversaries to purchase or acquire data to hinder states' ability to achieve national security objectives and

harm key elements of democratic societies. It is already possible to surveil and oppress individuals and groups in more obtrusive, less regulated ways. Censorship of Australians and Australian politicians by WeChat already occurs.[90] So does workplace monitoring,[91] private and public space monitoring, and crowd sourcing evidence of crimes,[92] where investigators collect critical information and leads from the public through social media. In future, we can expect the same tools to be used to facilitate espionage, interference, and other methods of interstate competition.

3. Big data drives information and political influence and interference

Big data can be used to harm individuals and society by providing mechanisms to improve information warfare as well as influencing and interfering in the political and civic discourse that is essential to democracy. The effectiveness of these capabilities is fuelled by datafication and made possible by using the mechanisms of targeted advertising known as "microtargeting".

British consulting firm Cambridge Analytica was implicated in a data breach connected to the 2016 US elections and attempted Russian interference in US elections *(Book Catalog/Flickr)*

Microtargeting, also referred to as personalisation, targeted digital advertising services, customer-targeted advertising, and precision targeting, is the use of data to target small groups or even individuals.[93]

The desire to target specific individuals with tailored messages — often advertising — is not new, but the technical capabilities underpinning this are being driven by the big data landscape and enabling contemporary information influence and interference.

To date, targeted advertising has largely been focused on developing new corporate revenue streams. However, it has the capacity to shape an individual's information environment, including what they see, the choices they are presented with, what they think others believe, and ultimately how they might view the world.[94] Fragmented media landscapes and microtargeting lead to an increase in political and social polarisation.[95] Microtargeting therefore presents significant national security threats. These include mass influence and interference, such as the ability to target specific groups, identify and exploit psychological weaknesses, and interfere in political and civil processes such as elections.

Fragmented media landscapes and microtargeting lead to an increase in political and social polarisation. Microtargeting therefore presents significant national security threats.

This kind of granular targeting is well established in the electoral and commercial realms[96] and has laid the groundwork for the kind of election influence and interference seen in recent years.[97] Examples include Cambridge Analytica's role in the 2016 US elections,[98] attempted Russian interference in US elections, [99] and Facebook's attempts to sell data on 6.4 million young Australians and New Zealanders claiming to identify their emotional state, particularly vulnerability and insecurity.[100] The effectiveness of microtargeting on individual behaviour is inconclusive[101] and unknown outside the big tech companies, which monetise their user data in this way. However, the use of political and commercial microtargeting, combined with a steady stream of big tech whistleblowers,[102] demonstrates the companies themselves are aware of its influence and potential.

Big data has exponentially accelerated the process and effectiveness of influence and interference, enabling it to occur at scale and at speed with increased opacity and ambiguity about intent or identification of who is behind the activity. Given the opaque nature of microtargeting processes — and their availability to anyone willing to fund campaigns — they are an ideal mechanism for grey zone information warfare.

CONCLUSION

The use of technology for influence and interference both at an individual and national scale has the power to challenge democratic principles and institutions.

Big data is a new frontier. We already know much about the improvements it has made to society. However, data abundance, digital connectivity, and ubiquitous technology continue to rapidly evolve and create new harms and national security threats. The big data landscape has embedded new structures for unprecedented collection and aggregation of data about almost every aspect of individuals' lives. Society is digitally connected at virtually every level and technology is ubiquitous in that connection.

The implications are still emerging, but it is clear that the landscape is changing for future Australians and for governments determined to deliver Australian security and prosperity. The big data landscape has concentrated data, technical, and analytical capabilities that are increasingly essential for functioning societies into the hands of a small number of commercial entities. This in turn has created new power dynamics between governments, citizens, companies, and nation states.

The national security threats related to the big data landscape are only beginning to surface. The use of technology for influence and interference both at an individual and national scale has the power to challenge democratic principles and institutions. Unless the risks are mitigated while the chance is available, they will proliferate into potentially uncontrollable problems.

However, despite a rapidly evolving threat environment, there is some cause for optimism. Societies have managed to regulate every significant industry in history — from railways, automobiles, and aviation to tobacco, pharmaceuticals, and food. The task now is to mitigate the most serious national security threats, ensure that growth and innovation of technologies reflect our values and culture, and manage big data and emerging digital technologies so that they improve democracy and the quality of societies.

ACKNOWLEDGEMENTS

This paper draws on PhD research conducted by the author at Deakin University. The thesis, *Big Data and National Security: Impacts for Intelligence* was supervised by Dr Chad Whelan. Publications are available at https://miahhe.com/phd. The PhD was supported by a National Security Big Data Scholarship from D2D CRC and a University Postgraduate Research Scholarship from Deakin University. Additional support was also provided by D2DCRC in the form of an Applied Research and Collaboration Award (2017) and an Applied Research Grant (2019). Thank you to the interviewees. It was a tremendous privilege and honour to interview the leaders and practitioners of Australia's National Intelligence Community and while they cannot be named, their time and insights are greatly appreciated. Hopefully, the PhD and this paper can do their contributions justice. Thank you to all reviewers for your helpful suggestions and improvements. Thank you to Lowy team for your wonderful work.

NOTES

Cover image: Gilles Lambert/Unsplash

[1] Rob Kitchin, "Big Data, New Epistemologies and Paradigm Shifts," *Big Data & Society*, Vol 1, Iss 1 (2014); *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences* (London: SAGE, 2014); Dennis Murphy and Daniel Kuehl, "The Case for a National Information Strategy," *Military Review*, September–October (2015), https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20151031_art013.pdf.

[2] Kitchin, "Big Data, New Epistemologies and Paradigm Shifts,"; Danah Boyd and Kate Crawford, "Critical Questions for Big Data," *Information, Communication & Society*, Vol 15, No 5 (2012), 662–79; and Miriam J. Metzger and Andrew J. Flanagin, "Credibility and Trust of Information in Online Environments: The Use of Cognitive Heuristics," *Journal of Pragmatics*, No 59, Part A (2013), 210–20.

[3] David Rubin et al., "Harnessing Data for National Security," *SAIS Review* 34, No 1 (2014).

[4] There are many different conceptualisations of national security. The notion of values is highlighted as "the absence of threats to acquired values and subjectively, the absence of fear that such values will be attacked" by Arnold Wolfers, *Discord and Collaboration; Essays on International Politics* (Baltimore, Johns Hopkins Press, 1962), 485. David A. Baldwin, "The Concept of Security," *Review of International Studies* 23 (1997), subsequently refined "the absence of threat" as "a low probability of damage to acquired values".

[5] Kitchin, *The Data Revolution*; Boyd and Crawford, "Critical Questions for Big Data".

[6] This paper draws on data collected as part of a larger research project that examined the impact of big data on intelligence production and national security in Australia. The research was conducted at Deakin University 2017–2021 and included ethics approval. It involved semi-structured interviews with 47 senior and operational decision-makers as well as technologists working in Australia's national intelligence community (NIC) agencies. The author gained access to some of Australia's most highly regarded intelligence leaders and practitioners to provide insight and analysis into the challenges and opportunities of big data. Intelligence practitioners are well positioned to provide insight into the

impact of big data on national security, however this paper extends beyond those conversations.

[7] Department of Defence., Defence Strategic Update, Department of Defence (Commonwealth of Australia, 2020), https://www.defence.gov.au/about/publications/2020-defence-strategic-update.

[8] Jacob Metcalf, Emily F. Keller, and Danah boyd, "Perspectives on Big Data, Ethics, and Society," (2016), 2.

[9] Boyd and Crawford, "Critical Questions for Big Data," 663.

[10] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data : A Revolution That Will Transform How We Live, Work, and Think*, First Mariner Books edition. ed. (Boston: Mariner Books, Houghton Mifflin Harcourt, 2014).

[11] Andrea De Mauro, Marco Greco, and Michele Grimaldi, "What Is Big Data? A Consensual Definition and a Review of Key Research Topics," American Institute of Physics Proceedings, (2015), 1644.

[12] Doug Laney, "3D Data Management Controlling Data Volume Velocity and Variety," *META Delta* File 949, 6 Febraruy 2001, https://studylib.net/doc/8647594/3d-data-management--controlling-data-volume--velocity--an...; Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*, 68.

[13] *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*, 68.

[14] Gregory B. Saathoff Babak Akhgar, Hamid R. Arabnia, Richard Hill, Andrew Staniforth, Petra Saskia Bayerl, *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies* (Amsterdam; Waltham Elsevier, 2015); Bart van der Sloot, Dennis Broeders and Erik Schrijvers, ed. *Exploring the Boundaries of Big Data* (The Hague: The Netherlands Scientific Council for Government Policy, 2016); and Rob Kitchin and Tracey P. Lauriault, "Small Data in the Era of Big Data," *GeoJournal* 80, No 4 (2014); Boyd and Crawford, "Critical Questions for Big Data"; Kitchin, "Big Data, New Epistemologies and Paradigm Shifts."

[15] The grouping of terms was first used by US intelligence leader Sue Gordon and in subsequent communication with the author she confirmed that to the best of her knowledge this grouping was her own construction. The same themes emerged in my research as features of big data most relevant to intelligence and my PhD offers empirical evidence to deepen understanding and define these terms.

[16] Kenneth Cukier, "Data, Data Everywhere," *The* Economist, 27 February 2010, https://www.economist.com/special-report/2010/02/27/data-data-everywhere.

[17] Jeff Desjardins, "How Much Data Is Generated Each Day?," World Economic Forum, 17 April 2019, https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/.

[18] David Reinsel, John Gantz, and John Rydning, "The Digitization of the World from Edge to Core," *Data Age 2025* (IDC White Paper, 2018), https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf. IDC predicts that the Global Datasphere will grow from 33 Zettabytes (ZB) in 2018 to 175 ZB by 2025.

[19] Customer Loyalty Schemes Review, Qantas Submission in Response to the ACCC's Draft Report, 3 October 2019, https://www.accc.gov.au/system/files/Qantas%20-%20October%202019.pdf; Andrew Curran, "Qantas Ready to Honor $3 Billion Worth of Frequent Flyer Miles", *Simply Flying*, 3 March 2021, https://simpleflying.com/qantas-3-billion-frequent-flyer-miles/.

[20] Qantas, "Privacy and Security," https://www.qantas.com/au/en/support/privacy-and-security.html.

[21] Mayer-Schönberger and Cukier, *Big Data*, 73–97.

[22] Kristene Unsworth, "The Social Contract and Big Data," *Journal of Information Ethics* 25, Spring (2016).

[23] Miah Hammond-Errey, "The Transformative Potential of Big Data," *The Interpreter*, 24 June 2019, https://www.lowyinstitute.org/the-interpreter/transformative-potential-big-data.

[24] David Omand and Mark Phythian, "Digital Intelligence and Cyberspace," ed. David Omand and Mark Phythian, *Principled Spying: The Ethics of Secret Intelligence* (Oxford University Press, 2018), 145.

[25] Georgia Dixon, "Aussies Spend Almost 17 Years in a Lifetime Staring at their Phones", *Reviews.org*, 7 April 2021, https://www.reviews.org/au/mobile/aussie-screentime-in-a-lifetime/.

[26] Hammond-Errey, "The Transformative Potential of Big Data."

[27] Shoshana Zuboff, "Creating Value in the Age of Distributed Capitalism," *McKinsey Quarterly*, 1 September 2010, https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/creating-value-in-the-age-of-distributed-capitalism; Unsworth, "The Social Contract and Big Data."; Tim Harford, "Big Data: Are We Making a Big Mistake?," *Financial Times*, 28 March 2014,

https://www.ft.com/content/21a6e7d8-b479-11e3-a09a-00144feabdc0; Michael J. Mazarr et al., "The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment," (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR2714.html.

[28] Kate Crawford and Jason Schultz, "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms," *Boston College Law Review* 55, No 1 (2014), https://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4/; Australian Government, "What Is Personal Information?," (Canberra, Australia: Office of the Australian Information Commissioner, 2017), https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information.

[29] See for example, L. Rocher, J. M. Hendrickx, and Y. A. de Montjoye, "Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models," *Nature Communications* 10, No 1 (2019), https://www.nature.com/articles/s41467-019-10933-3; Ira S. Rubinstein and Woodrow Hartzog, "Anonymization and Risk," *Washington Law Review* 91 (2016), https://digitalcommons.law.uw.edu/wlr/vol91/iss2/18/; Y. A. de Montjoye et al., "Unique in the Crowd: The Privacy Bounds of Human Mobility," *Nature Communications Rep* 3 (2013), https://www.nature.com/articles/srep01376.pdf.

[30] Henrik Twetman and Gundars Bergmanis-Korats, "Data Brokers and Security," *Risks and Vulnerabilities Related to Commercially Available Data* (NATO StratCom COE, 2021), https://stratcomcoe.org/publications/data-brokers-and-security/17; Dymples Leong and Teo Yi-Ling, "Data Brokers: A Weak Link in National Security," *The* Diplomat, 21 August 2020, https://thediplomat.com/2020/08/data-brokers-a-weak-link-in-national-security/; Matthew Crain, "The Limits of Transparency: Data Brokers and Commodification," *New Media & Society* 20, No 1 (2016); Kitchin, *The Data Revolution*.

[31] Crain, "The Limits of Transparency: Data Brokers and Commodification."

[32] Twetman and Bergmanis-Korats, "Data Brokers and Security."; Leong and Yi-Ling, "Data Brokers: A Weak Link in National Security."; Crain, "The Limits of Transparency: Data Brokers and Commodification."; Kitchin, *The Data Revolution*.

[33] "What Are Data Brokers — And What is Your Data Worth?", WebFX, 16 March 2020, https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/.

[34] Murat Sonmez, "How Data Exchanges Can Level the Digital Playing Field," World Economic Forum, 28 June 2019, https://www.weforum.org/agenda/2019/06/data-exchanges-digital-ai-artificial-intelligence/.

[35] Gareth Mitchell, "How Much Data Is on the Internet?," *BBC Science Focus* Magazine, 2019, https://www.sciencefocus.com/future-technology/how-much-data-is-on-the-internet/.

[36] Twetman and Bergmanis-Korats, "Data Brokers and Security."

[37] Ibid.

[38] "World's Biggest Data Breaches & Hacks", Information is Beautiful, Accessed October 2021, https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

[39] "Bridging the World through Digital Connectivity," StoryWorks, BBC (2018), https://www.bbc.com/storyworks/specials/digital-connectivity/.

[40] Klaus Schwab, *The Fourth Industrial Revolution* (Penguin Books Limited, 2017).

[41] Ibid.

[42] Australian Government Productivity Commission, "Digital Disruption: What Do Governments Need to Do?," Productivity Commission Research Paper (Canberra: Australian Government Productivity Commission, 2016), https://www.pc.gov.au/research/completed/digital-disruption.

[43] Surjit Singh and Rajeev Mohan Sharma, *Handbook of Research on the Iot, Cloud Computing, and Wireless Network Optimization* (IGI Global, 2019); Intel, "A Guide to the Internet of Things," https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html.

[44] Murphy and Kuehl, "The Case for a National Information Strategy," 72.

[45] Intel, "A Guide to the Internet of Things".

[46] Unsworth, "The Social Contract and Big Data."

[47] There is extensive research revealing that many of the categorisation methods and inferences and assumptions made about humans and human behaviour using big data and AI are not technically sophisticated, are unsubstantiated, and in some cases simply untrue. See for examples, Kate Crawford and Jason Schultz, "AI Systems as State Actors," *Columbia Law Review*, Vol 119, No 7, https://columbialawreview.org/content/ai-systems-as-state-actors/; Kate Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, (Yale University Press 2021);

and Huon Curtis, "Finding Australia's Asymmetric Advantage in Big Data", *The Strategist*, ASPI, 30 June 2021, https://www.aspistrategist.org.au/finding-australias-asymmetric-advantage-in-big-data/.

[48] Genevieve Bell, "The Character of Future Indo-Pacific Land Forces," *Australian Army Journal* XIV, No 3 (2018), 175, https://search.informit.org/doi/pdf/10.3316/ielapa.377081144168780.

[49] José van Dijck, Thomas Poell, and Martijn de Waal, *The Platform Society: Public Values in a Collective World* (Oxford Scholarship Online, 2018).

[50] Ibid.

[51] Mazarr et al., "The Emerging Risk of Virtual Societal Warfare."; Shosana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: Barack Obama's Books of 2019* (Profile, 2019); Dale Neef, "Big Data Big Bang," ed. Dale Neef, *Digital Exhaust: What Everyone Should Know About Big Data, Digitization, and Digitally Driven Innovation* (PH Professional Business, 2014); Meredith Whittaker, "The Steep Cost of Capture," *Interactions* XXVIII, November–December 2021 (2021).

[52] van Dijck, Poell, and de Waal, *The Platform Society*; Rodrigo Fernandez, Tobias J. Klinge, Reijer Hendrikse, and Ilke Adriaans, "How Big Tech Is Becoming the Government," *Tribune Magazine*, 5 February 2021, https://tribunemag.co.uk/2021/02/how-big-tech-became-the-government.

[53] Mazarr et al., "The Emerging Risk of Virtual Societal Warfare."

[54] Omand and Phythian, "Digital Intelligence and Cyberspace," 145.

[55] Jayshree Pandya, "The Dual-Use Dilemma of Artificial Intelligence," *Forbes*, 28 January 2019, https://www.forbes.com/sites/cognitiveworld/2019/01/07/the-dual-use-dilemma-of-artificial-intelligence/?sh=748ef99d6cf0.

[56] Carissa Véliz, "Privacy and Digital Ethics after the Pandemic," *Nature Electronics* 4, No 1 (2021).

[57] Digital Advertising Services Inquiry 2020–2025: Interim report, ACCC, https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-2025.

[58] New Media Bargaining Code, ACCC, 2020, https://www.accc.gov.au/focus-areas/digital-platforms/news-media-bargaining-code; Peter Lewis, "Facebook's Capitulation in Australia is the Beginning of the Project to Regulate Big Tech – Not the End, *The Guardian*, 23 February 2021, https://www.theguardian.com/media/2021/feb/23/facebooks-

capitulation-in-australia-is-the-beginning-of-the-project-to-regulate-big-tech-not-the-end.

[59] John Lee, "Big Data for Liberal Democracy," *The Australian*, 5 March 2021, https://www.theaustralian.com.au/inquirer/big-data-for-liberal-democracy/news-story/10ed6d4d8b01677955fc468d3751a4b7.

[60] Ibid.

[61] Cristian Santesteban and Shayne Longpre, "How Big Data Confers Market Power to Big Tech: Leveraging the Perspective of Data Science," *The Antitrust Bulletin* 65, No 3 (2020).

[62] Joanna Redden, "Six Ways (and Counting) That Big Data Systems Are Harming Society," *The Conversation*, 7 December 2017, https://theconversation.com/six-ways-and-counting-that-big-data-systems-are-harming-society-88660.

[63] Department of Defence, "Defence Strategic Update."

[64] Ibid.

[65] Véliz, "Privacy and Digital Ethics after the Pandemic."

[66] Anja Prummer, "Micro-Targeting and Polarization," *Journal of Public Economics* 188, August, (2020). Julie E. Cohen, "Law for the Platform Economy," *University of California, Davis Law Review* 51 (2017).

[67] ASIO, *Asio Annual Report 2019–20*, Commonwealth of Australia, 2020, 3-4, https://www.asio.gov.au/sites/default/files/ASIO%20Annual%20Report%202019-20.pdf.

[68] ASIO, *Director-General's Annual Threat Assessment*, Wednesday 17 March 2021, https://www.asio.gov.au/publications/speeches-and-statements/director-generals-annual-threat-assessment-2021.html.

[69] Ibid.

[70] Ibid.

[71] ASIO, *Asio Annual Report 2019–20*, 4.

[72] Ibid., 3-4.

[73] Danielle Cave, "Data Driven: How Covid-19 and Cyberspace Are Changing Spycraft," *Australian Foreign Affairs*, Spy vs Spy The New Age of Espionage, No 9 (2020), https://www.australianforeignaffairs.com/articles/extract/2020/07/data-driven.

[74] ASIO, *Director-General's Annual Threat Assessment,* 2021.

[75] Martin C. Libicki, "Information Dominance," *Strategic Forum Institute for National Strategic Studies and the National Defense University* 132 (1979).

[76] J. Michael Dahm, "Exploring China's Unmanned Ocean Network," *Asia Maritime Transparency Initiative*, 16 June 2020, https://amti.csis.org/exploring-chinas-unmanned-ocean-network/.

[77] Ibid.

[78] Entities are added to the US Entity List when it is determined they are acting contrary to the national security or foreign policy interests of the United States.

[79] Dahm, "Exploring China's Unmanned Ocean Network."

[80] Elsa B. Kania, "Chinese Military Innovation in Artificial Intelligence," Testimony before the US–China Economic and Security Review Commission Hearing on Trade, Technology, and Military–Civil Fusion, Center for New American Security, 7 June 2019, https://www.cnas.org/publications/congressional-testimony/chinese-military-innovation-in-artificial-intelligence.

[81] J. Michael Dahm, "Introduction to South China Sea Military Capabilities Series," *South China Sea Military Capabilities Series: A Survey of Technologies and Capabilities on China's Military Outposts in the South China Sea* (The Johns Hopkins University Applied Physics Laboratory, 2020), https://www.jhuapl.edu/Content/documents/IntroductiontoSCSMILCAPStudies.pdf.

[82] H. I. Sutton, "China Builds Surveillance Network in South China Sea," *Forbes*, 5 August 2020, https://www.forbes.com/sites/hisutton/2020/08/05/china-builds-surveillance-network-in-international-waters-of-south-china-sea/?sh=5f3d462174f3.

[83] John Gray, "Surveillance Capitalism Vs. The Surveillance State," *Noema*, 17 June 2020, https://www.noemamag.com/surveillance-capitalism-vs-the-surveillance-state/.

[84] Ibid.

[85] ACCC, "Digital Advertising Services Inquiry: Interim Report 2020, 56.

[86] Mayer-Schönberger and Cukier, *Big Data*, 73–97.

[87] The Xinjiang Data Project, Australian Strategic Policy Institute, https://xjdp.aspi.org.au.

[88] Dana Priest, Craig Timberg, and Souad Mekhennet, "Private Israeli Spyware Used to Hack Cellphones of Journalists, Activists Worldwide," *The*

Washington Post, 18 July 2021, https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/.

[89] Kitchin, *The Data Revolution*; Crain, "The Limits of Transparency".

[90] Fergus Ryan, "Censorship Risks and Electoral Impact: Australia's Major Parties Need to Drop WeChat", *The Strategist*, 10 December 2020, https://www.aspistrategist.org.au/censorship-risks-and-electoral-impact-australias-major-parties-need-to-drop-wechat/.

[91] Darrell M. West, "How Employers Use Technology to Surveil Employees," Brookings, 5 Janaury 2021, https://www.brookings.edu/blog/techtank/2021/01/05/how-employers-use-technology-to-surveil-employees/.

[92] David Omand, Jamie Bartlett, and Carl Miller, "Introducing Social Media Intelligence (Socmint)," *Intelligence & National Security* 27, No 6 (2012).

[93] Michael J. Mazarr et al., "Hostile Social Manipulation: Present Realities and Emerging Trends," (Santa Monica, California RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR2713.html.

[94] Ibid.; Miah Hammond-Errey, "Understanding and Assessing Information Influence and Foreign Interference," *Journal of Information Warfare* 18, Winter (2019); Richmond, "A Day in the Life of Data."

[95] Prummer, "Micro-Targeting and Polarization."

[96] "Digital Microtargeting Political Party Innovation Primer 1," International Institute for Democracy and Electoral Assistance IDEA, (Stockholm,: International Institute for Democracy and Electoral Assistance, 2018); Mazarr et al., "Hostile Social Manipulation: Present Realities and Emerging Trends."

[97] Mazarr et al., "Hostile Social Manipulation"; and Mazarr et al., "The Emerging Risk of Virtual Societal Warfare."

[98] Barbara Trish, "Big Data under Obama and Trump: The Data-Fueled US Presidency," *Politics and Governance* 6, No 4 (2018).

[99] Mazarr et al., "The Emerging Risk of Virtual Societal Warfare."

[100] A document leaked from Facebook's Australian office in 2017 showed analysis of internal (non-public) Facebook data that attempted to identify emotionally vulnerable and insecure young people to "give them a confidence boost". The document was to be shared with advertisers under a non-disclosure agreement and noted that Facebook had the power to target over 6.4 million Australian and New Zealander high schoolers, tertiary students, and young people in the workforce. Using its

algorithms to monitor newsfeed posts and photos as well as a young user's interaction with content through comments, likes, and shares, Facebook detailed in the report how it was able to ascertain a person's emotional state — categorising them with tags such as "anxious", "nervous", "defeated", "stressed" and "useless". Nick Whigham, "Leaked Document Reveals Facebook Conducted Research to Target Emotionally Vulnerable and Insecure Youth," *news.com.au*, 1 May 2017, https://www.news.com.au/technology/online/social/leaked-document-reveals-facebook-conducted-research-to-target-emotionally-vulnerable-and-insecure-youth/news-story/d256f850be6b1c8a21aec6e32dae16fd; and Peter Griffin, "Facebook Won't Give up Its Insidious Practices without a Fight," *Noted*, 22 March 2019.

[101] For discussion of the complexities relating to political microtargeting, see for example, Brahim Zarouali, Tom Dobber, Guy De Pauw, and Claes De Vreese, "Using a Personality-Profiling Algorithm to Investigate Political Microtargeting: Assessing the Persuasion Effects of Personality-Tailored Ads on Social Media, *Communication Research*, 20 October 2020.

[102] The most recent, Frances Haugen from Facebook, joined a growing list of Silicon Valley whistleblowers. See for example Johana Bhuiyan, "'Welcome to the Party': Five Past Tech Whistleblowers on the Pitfalls of Speaking Out", *The Guardian*, 9 October 2021, https://www.theguardian.com/technology/2021/oct/08/tech-whistleblowers-facebook-frances-haugen-amazon-google-pinterest.

ABOUT THE AUTHOR

Miah Hammond-Errey

Miah Hammond-Errey has more than 15 years of experience leading tactical, operational, and strategic analysis and communications activities for the Australian government and has represented Australia overseas in Europe and Asia. She is a Senior Analyst at ASPI's International Cyber Policy Centre. Her PhD from Deakin University examined the impact of big data on intelligence production and national security in Australia. This research was supported by a National Security Big Data Scholarship from Data 2 Decisions CRC and a Deakin University Postgraduate Research Scholarship. Miah has a Master of National Security Policy (Advanced) with Honours from the Australian National University, a Master of Criminology from Sydney University Law School, and a Bachelor of Arts from Sydney University.

LOWY INSTITUTE

31 Bligh Street
Sydney NSW 2000

Tel. +61 2 8238 9000
Fax +61 2 8238 9005

lowyinstitute.org
@LowyInstitute