Volume **6** (1) 2024 https://doi.org/10.5204/lthj.3256

Government and Commercial Interests in Genomics: Improving Data Security and Regulation

Marcus Smith
Charles Sturt University, Australia
Ausma Bernot
Griffith University, Australia

Abstract

The relationship between new technologies and security is well established in the fields of defence, law enforcement, communications and public health. This has been highlighted by recent public debate about the security implications of data held by companies operating in social media and information technology (such as TikTok and Huawei). While genomic technology had been less high profile in the context of security, this changed following the COVID-19 pandemic, which focused attention on the significant implications of this form of data. This article discusses commercial genomic technology, related government interests and the growing implications for data security and regulation, such as through the example of the Beijing Genomics Institute, a large company providing genomic testing services to consumers worldwide. We suggest that commercial genomic data has growing implications for countries such as the United States and Australia and argue for greater attention to be directed to this form of technology and associated data security and regulation, including security assessment to address the risks associated with international transfer via corporate entities.

Keywords: Genomics; genomic technology; genomic data security; technology regulation; international security; surveillance.

1. Introduction

Technology advancement has long been linked with economic development, international security and military superiority.[1] However, the field of genomics and its international security implications has received less attention in the literature until recently. In a 2021 assessment, the US Office of the Director of National Intelligence warned that 'losing your DNA is not like losing a credit card. You can order a new credit card but you cannot replace your DNA.'[2] This was followed in 2022 by the US Department of Defense identifying six Chinese genomics companies as 'military companies operating in the United States'.[3] Specifically, China's genomic industry has been identified as a threat to national security, with a focus on the company Beijing Genomics Institute (BGI), a national leader in this field of research in China and one of the largest exporters of genomic products internationally. This article explores genomic data security governance and regulation considerations in the United States and Australia, in the context of Chinese genomics sales increasingly being narrated as threats of national security.

[1] Vogel and Ouagrham-Gormley, "Anticipating Emerging Biotechnology Threats."
[2] National Counter-intelligence and Security Center, "China's Collection of Genomic and other Healthcare Data from America."
[3] US Department of Defense, "Entities Identified as Chinese Military Companies."

The transnational exchange of corporate genomic data is occurring in the context of an increasing focus on cyber and data security. This comes at a time when the 'strategic trust' between Western countries and countries such as China has been diminished, especially in relation to data security and its potential to be used in the future in contexts such as 'hacktivism,' cybercrime, cyber-espionage and cyberwarfare.[4] The genomics sector is predicted to grow in both scale and sophistication due to large government and private investments in the industry.[5] While China and India are growing in importance in contemporary life sciences, including genomics, their rise also reflects the multitude of regulatory challenges for science governance shared globally.[6] Of particular concern is China's military development strategy, known as military–civil fusion.[7] While some scholars warn against the simplistic linking of China's genomic development with immediate conversion to genetic weaponry,[8] national security concerns continue to dominate international reactions to China's genomics industry.

Data security issues have been raised in relation to the activities of several companies operating in the United States, Australia and elsewhere, with the association between the state and commercial sectors a key issue.[9] Security issues have been raised in relation to products across several fields, including 5G infrastructure. One example is the social media company TikTok's potential to share data with the Chinese government, which has been the subject of parliamentary inquiries and media.[10] The use by government departments of China-made CCTV surveillance cameras, manufactured by Dahua and Hikvision, has led to debate over whether a more comprehensive approach is needed to evaluate Chinese technologies and their potential data privacy and security risks.[11] It should also be acknowledged that relationships between the corporate sector, including social media and technology companies, and intelligence agencies, have been documented in liberal democracies, as evidenced by Edward Snowden's disclosures.[12] Further, as will be discussed in greater detail later, genomics companies in the United States, such as GEDMatch and 23andMe collaborate with law enforcement agencies through a technique known as forensic investigative genetic genealogy, in which their customers' data is used to solve serious crimes.[13]

Considerations of national security are increasingly influencing economic decision-making, with growing recognition that national security and the economy are interrelated.[14] Cave argues that the Australian Government should develop a comprehensive approach to evaluating security challenges rather than approaching them as independent issues.[15] Recent developments in relation to Australia's trade relationships have highlighted the links between economics and national security, and the vulnerability of Australia's relatively small economy.[16] The genomics sector is growing rapidly, and will face even greater commercial and security implications in the years ahead.

Genomic data represents a growing and underappreciated security threat as it is generated and applied increasingly widely in health and ancestry contexts. It can provide strategically significant information about individuals and populations, and alongside current developments in artificial intelligence, genomic technologies may have the most significant implications for humanity of any technology currently being developed. Genomic data is most often created for medical, population health and genealogy purposes. Its uses can include disease diagnosis, the provision of medical treatment, medical research or recreational ancestry. As we saw during the COVID-19 pandemic, genomic data also has security implications. It can play a key role in creating and responding to biological threats, such as COVID-19 genome sequencing, used to track mutations and identify chains of transmission.[17] Through the field of DNA evidence, it also has a decades-long history of use within the criminal justice system, where it has played a major role in identifying individuals and contributing to public security and law enforcement.[18]

As genome sequencing has become more efficient and cheaper to undertake, the volume of data that can be generated and analysed for security and health purposes has increased markedly.[19] Consequently, the significance of the collection has grown,

[4] Hartcher, "Huawei? No way!" Simon, "Critical Infrastructure and the Internet of Things."
[5] Moore, "China's Role in the Global Biotechnology Sector and Implications for U.S. Policy."
[6] Zhang, "The Elephant and the Dragon in Contemporary Life Sciences."
[7] Kania, "China's Military Biotech Frontier."
[8] Vogel, "Anticipating Emerging Biotechnology Threats."
[9] Depoux, "Can Chinese Giants Become Multinational Companies?"
[10] Parliament of Australia, "Select Committee on Foreign Interference Through Social Media."
[11] Bernot,"Understanding the risks of China-made CCTV Surveillance Cameras in Australia."
[12] Dencik, "The Advent of Surveillance Realism."
[13] Smith, "A Principled Approach to Cross-Sector Genomic Data Access."
[14] Golley, "Geoeconomics and the Australian University Sector: A 'Geoeducation' Analysis."
[15] Cave, "Huawei and Australia's 5G Network."
[16] Ferguson, "Economic Power and Vulnerability in Sino-Australian Relations."
[17] Australian Academy of Science, "Genome Sequencing COVID-19."
[18] Smith, DNA Evidence in the Australian Legal System.
[19] Satam, "Next-generation Sequencing Technology: Current Trends and Advancements."

as have the analytic and application capabilities. This is compounded by the increased scale of genomic databases, increasing the risk and potential impact of data breaches. For example, in 2018 the MyHeritage data breach exposed sensitive genomic data of 92 million users via a leaked file containing email addresses and hashed passwords.[20]

This article argues that there are interrelated developments in the international security implications of commercial genomic data that necessitate regulatory reforms. Section 2 discusses the data security implications of genomics. Section 3 describes commercial genomics in China and its strategic significance. Section 4 examines BGI, and the security concerns associated with its provision of genomic testing to consumers around the world. Section 5 argues that the emerging national security concerns and implications of genomics, as evidenced by current security assessments, require steps to be taken to mitigate the threat.

The argument that unfolds throughout the article seeks to highlight the fact that greater regulatory scrutiny must be directed to the issue of genomic data security. Recent developments in the commercial genomics industry are important, both now and into the future. They provide reasons to carefully consider the potential end uses of the genomic data, for governments to investigate the more stringent regulation of their citizens' data and for genomic data to be viewed as a key national resource. Companies providing commercial genomic products and services should be vetted and regulated, and if it is appropriate for them to do so, required to securely store genomic data. Governments should be cognisant of the ramifications of offshore movement of this data. Developments in commercial genomics illustrate the need for a more comprehensive approach by the Australian Government to evaluate the security risks associated with the genomic data of Australian citizens and address them.

2. Genomics and Security

Genomics involves the analysis of the entire human genome; this is in contrast to genetics, the analysis of single genes and how traits are passed on to following generations.[21] Genomic data are sensitive and can reveal an individual's identity, health status, susceptibility to disease, ethnicity, paternity and relatedness. Perhaps the earliest collection of this form of data was via 'Guthrie', or newborn screening, cards, an approach that has been undertaken for all births in Australia and most other developed countries for approximately half a century. It involves the collection, storage and screening of babies' blood within a few days of birth, and associated testing for a range of genetic conditions, such as cystic fibrosis.[22] Genomic technologies are becoming increasingly important to medical research and treatment, and the field has developed and continued to expand following the completion of the Human Genome Project in 2003 by the US Department of Energy and the National Institutes of Health, which located and sequenced all human genes. More recently, genomics has benefited from advancements in big data analytics and artificial intelligence, and its influence on human health and clinical medicine will continue to grow.[23] The Human Genome Organization's Imagined Futures initiative describes likely future issues for genomics, which include data security and privacy, consent, expanded usage, human error, hacking and interoperability of storage formats.[24]

As is the case across a number of sectors, data security in healthcare is becoming a more significant issue for governments and individuals as new forms of data are generated, and in greater volumes. The threat of cybersecurity is now well understood as instances of data breaches involving national institutions, governments and businesses become more common. Whether the data are held in the public or private sector, genomic databases provide a rich source of information relating to individuals and populations. This is not only key to medical treatment and research, but can be used to understand and identify people, link them with their relatives and determine population-specific vulnerabilities.[25]

Genomic analysis can diagnose specific diseases, provide predictive health screening, identify predispositions to specific diseases to inform lifestyle choices and facilitate ancestry tracing to ascertain the ethnic background of a person and identify their genetic relatives. Comprehensive databases of citizens' genomic data have the potential to create power imbalances between governments and citizens,[26] and the regulation of this data is important to maintain rights such as privacy and autonomy.[27]

[20] Wong, "Characterizing the Harms of Compromised Genetic Information for Article III Standing in Data Breach Litigation."
[21] World Health Organization, "Human Genomics in Global Health."
[22] Bowman, "Newborn Screening Cards."
[23] Oliveira, "Biotechnology, Big Data and Artificial Intelligence."
[24] Capps, "Statement on Bioinformatics."
[25] Mittal, "Digital Health."
[26] Qiang, "The Road to Digital Unfreedom."
[27] Wan, "Sociotechnical Safeguards for Genomic Data Privacy."

The All of Us program in the United States, which is planning to sequence the genomes of a million Americans, and the 100,000 Genomes Project in the United Kingdom are population-wide databases that seek to harness national health benefits from genomic data and inform medical research. They will contribute to new interventions and improved public health planning.[28] The potential healthcare benefits of genomics range from new therapies and personalized medicine to better public health policy, surveillance during pandemics and preventative vaccines. Big data and artificial intelligence will have an impact on most areas of society, including the analysis of genomic data to deliver more precise healthcare. Healthcare benefits can also be security benefits, as in the case of vaccines against infectious diseases, as illustrated by COVID-19. The pandemic clearly demonstrated that genomics is associated with risks that threaten international security, potentially undermining economic and political stability across the world. The potential to leverage human population and pathogen genomic data with emerging techniques such as CRISPR highlights these risks.[29]

The financial incentive to commercialize new technology has led to the emergence of online, direct-to-consumer (DTC) genomics companies that offer mail-order testing for health conditions and ancestry. Since the mid-2000s, they have offered an increasing range of services.[30] Companies headquartered in the United States include 23andMe, Ancestry.com and GEDmatch, which enable users to upload data from multiple providers and search for their genetic relatives.[31] These companies' services are widely used, and as the cost of the technology has become cheaper, the price of services has reduced; the customer base of the leading companies is in the tens of millions worldwide, and growing each year.[32]

The aggregate value of DTC genomics company data sets is now significant from the perspectives of pharmaceutical companies, medical researchers, government agencies and law enforcement. 23andMe, which provides 'genetic risk tests' for a range of conditions, including Alzheimer's disease and Parkinson's disease, shares aggregate information about the prevalence of genetic traits in their customers as part of its business. In 2018, pharmaceutical company GlaxoSmithKline invested $300 million in 23andMe for the purpose of using customers' deidentified aggregate data for research purposes.[33] It also shares identifiable genomic data about individuals, as required by laws, regulations and judicial requirements.[34]

The security benefits of genomic data include the establishment and use of increasingly sophisticated DNA databases, and techniques to identify criminal offenders and exculpate those who are innocent. The forensic use of DNA has a decades long history in the criminal justice system. This form of genomic analysis can identify individuals with a high degree of accuracy and link them with crimes through biological evidence. Forensic geneticists are now utilizing new applications of genomic analysis, such as screening a suspect's sample to determine their likely physical appearance, a practice known as forensic phenotyping.[35]

The cross-sector use of genomic health and ancestry data by law enforcement in criminal investigations in the United States has been well documented. If, in an investigation of a serious crime, a law enforcement agency is not able to obtain a match for a suspect's DNA profile on their national forensic DNA database, they may search a commercial genomic database for a relative of their suspect.[36] This technique is known as Forensic Investigative Genetic Genealogy, and it is much broader in scope than matching against a forensic DNA database of convicted offenders that is regulated by criminal procedures legislation. It facilitates searching of up to fourth cousins (often around 100 people) of the person that submitted their genomic data to a direct-to-consumer testing company.[37] Given that it is estimated that tens of millions of people have submitted their genomic data for testing to one of these companies, it has a vast potential scope as an investigative technique, to the extent that anyone in developed countries can now potentially be identified.[38] We should acknowledge that there are significant security risks associated with this data and that there is a need for greater regulation to ensure it is only used for lawful purposes, and to ensure it is stored securely.

[28] Feero, Precision Medicine, Genome Sequencing."
[29] Vogel, "China's Biomedical Data Hacking Threat."
[30] Commercial ancestry databases are also referred to as recreational genealogical databases.
[31] See, for example, 23andMe www.23andme.com; Ancestry www.ancestry.com; Family Tree DNA www.familytreedna.com; GEDMatch www.gedmatch.com.
[32] Regalado, "China's BGI Says It Can Sequence a Genome for Just $100."
[33] Wang, "Big Pharma Would Like Your DNA."
[34] 23andMe Privacy Policy, section 4(e).
[35] Smith, Technology Law: Australian and International Perspectives.
[36] Smith, "A Principled Approach to Cross-Sector Genomic Data Access."
[37] Smith, "A Principled Approach to Cross-Sector Genomic Data Access."
[38] Miller, "Quasi Universal Forensic DNA Databases."

3. Commercial Genomics in China

The Chinese Government has invested heavily in emergent technologies, including those relating to artificial intelligence, biotechnology, and cybersecurity. China's party-state merges its social control interests with the profit-seeking interests of the private sector. It is reasonable to assume that large private companies are to some extent affiliated with the Chinese party-state. Since the 1970s, when China's market opened up, the country's market system has evolved into 'party-state capitalism'.[39] For many companies in China, aligning the goals of the company with those of the party-state is a well-established business strategy, often linked with strategic business development opportunities.[40]

As occurs in many countries, Chinese companies foster strategic political connections to obtain government funding and access to commercial networks.[41] The national intelligence law may require them to provide corporate data to the state, where it is considered by the government to be relevant to the national interest.[42] Due to the communist state framework of the political system, the government can exert greater control over companies than in the West. BGI has been well supported by the Chinese government for many years. For example, after outlining a plan for sequencing the human genome in 1999, BGI has received both political and financial support from the government, including the selection of BGI's co-founder as a member of the Chinese Academy of Sciences, as well as large strategic loans and grants that have supported the rapid growth and scaling of the company.[43] In its initial public offering documentation, BGI reported over CNY 1 million in government grants to support the company's projects in technology park building, cancer screening, bioengineering and new pharmaceutical development, among other business and research activities.[44]

Genomic data is strategically significant to the Chinese government. In 2016, China's party-state launched the National GeneBank (国家基因库), with the intention of developing it into the world's largest repository of genomic data. Its stated aim is to 'develop and utilize China's valuable genetic resources, safeguard national security in bioinformatics (生物信息学), and enhance China's capability to seize strategic heights in the domain of biotechnology'.[45] A push to develop genomic technologies was outlined in the 13th Five-Year Plan (2016–2020). It sought to develop the biotechnology industry in a number of ways, including by:

- accelerating the wide application of genomics and other biotechnologies
- creating demonstrations of network-based biotech applications
- promoting large-scale development of personalized medical treatments, new drugs, bio-breeding and other next generation biotech products and services, and
- promoting the creation of basic platforms such as gene and cell banks.[46]

The 14th Five-Year Plan (2021–2025) continues this focus. Gene technology and biotechnology are one of the seven frontier fields of science and technology, and biotechnology is classified as one of the country's strategic emerging industries.[47] These mid- to long-term plans also include clear provisions for military–civilian integration, along with advancement in other key areas, such as quantum technology, new materials and intelligent remotely piloted systems.[48] Commentators in other countries, such as Australia, have expressed concerns about the links between the worldwide collection of commercial data and military research in China, not only in relation to genomics but in other areas, such as social media and artificial intelligence (AI), that may indicate that data collection in this sector is part of a broader trend.[49]

[39] Pearson, "China's Party-State Capitalism and International Backlash."
[40] Bernot, "Understanding the Risks of China-made CCTV Surveillance Cameras in Australia."
[41] Bernot, "Understanding the Risks of China-made CCTV Surveillance Cameras in Australia."
[42] Girard, "The Real Danger of China's National Intelligence Law."
[43] Wang, "Sequencing BGI."
[44] BGI "Initial Public Offering and Listing on the GEM Prospectus."
[45] China.org, "China's First Gene Bank to Open in Shenzhen."
[46] National Development and Reform Commission of the People's Republic of China, "The 13th Five-year Plan for Economic and Social Development of the PRC."
[47] Huada Genomics, "From Technological Innovation to Internationalisation Upgrade, Creating a Sample of Precision Medicine Industry."
[48] China National Defense Science and Technology Information Center, "The Full Text of the '13th Five-Year Plan' Special Plan for the Development of Military–Civilian Integration of Science and Technology."
[49] Australian Strategic Policy Institute, "Mapping China's Tech Giants."

China's bioinformatics infrastructure has previously been raised by scholars as a means of obtaining a more holistic view of how genomic data might be used in practice by governments in the future.[50] BGI occupies an important role as a major global genomics company in China's bioinformatics landscape, distinguishing itself for its extensive DNA sequencing capacity at low cost (BGI was first to break the US$100 mark for human genome sequencing), and has created a significant portion of the world's genomic data.[51] Chinese researchers actively participate in bioinformatics, from large-scale genomic analysis to algorithm development, as reflected in a large number of publications in leading journals.[52] The Chinese government recognizes the future importance of bioinformatics and genomics research, and provides funding and support for further initiatives in the field, such as the genome sequencing archive.[53] Vogel and Ouagrham-Gormley (2022) highlight the need for further research and analysis into these issues:

We need to do a better job of conducting more complex socio-technical assessments of how China might try to use biomedical big data, as well as studying China's bio-informatics personnel and technical infrastructure. Just focusing on the data and the people who steal them does not tell us enough about China's ability to use those data for economic or security purposes. Security concerns about biomedical big data (and China's role in biomedical data hacking) need to be further studied and scrutinized with more robust empirical evidence in order to better inform U.S. decision-makers about the true nature of China's economic and national security threats.[54]

Significant international security concerns are associated with the genomic data held by Chinese companies due to the relationship between the industry and the state, and these are beginning to be appreciated by western democracies. In the following section, we examine the Chinese security environment and BGI more closely.

4. Beijing Genomics Institute

BGI is the national leader in China's genomics industry. Founded in 1999, it now has over 6000 employees worldwide and its business spans the agriculture, conservation and environmental sectors, as well as healthcare. The total value of the company was estimated at approximately US$8 billion in its 2021 investor report.[55] Its aim is to 'make state-of-the-art genomics highly accessible to the global research community', with a focus on large-scale and large-throughput genomic applications.[56] BGI's low cost and efficient gene-sequencing business has amassed customers around the world and accumulated a large volume of genomic data. The company's products have attracted attention from national security stakeholders and media reporting on alleged data harvesting practices in 2021.[57] In 2020, BGI reported receiving approximately US$8 million in Chinese government subsidies.[58]

Internationally, BGI has been best known for its prenatal testing products, although it is expanding its range of services. While it also offers whole genome sequencing services to customers worldwide, it is one of the few companies that has developed a non-invasive prenatal test (NIPT) for a disease known as foetal trisomy.[59] NIPTs test foetal cell-free DNA fragments in the peripheral blood of pregnant women. Since the 2010s, they have replaced invasive procedures in neonatal testing, which carry an increased risk of miscarriages. In 2020, Australia and fourteen European countries adopted NIPT as part of national testing programmes.[60] BGI's NIFTY (Non-Invasive Fetal TrisomY) test is a whole genome-based NIPT that can detect trisomy 21 (Down Syndrome), trisomy 18 (Edwards Syndrome), trisomy 13 (Patau Syndrome) and other chromosomal abnormalities.[61]

The NIFTY test comes at a low investment cost to laboratories overseas, as they are not required to purchase their own instruments, but simply collect and ship samples for analysis. After blood samples are extracted from a patient, they are sent to laboratories in either Hong Kong or Thailand, and from there test results are delivered online to the patient or clinician.[62]

[50] Vogel, "Anticipating Emerging Biotechnology Threats."
[51] Regaldo, "China's BGI Says it Can Sequence a Genome for just $100."
[52] Wei, "Bioinformatics in China"; Zhang and Liao, "Behind the Rising Influence of Chinese Research."
[53] Xia, "Biopharma CRO Industry in China."
[54] Vogel, "China's Biomedical Data Hacking Threat."
[55] Vogel, "China's Biomedical Data Hacking Threat."
[56] BGI Group, Annual Report 2020.
[57] Needham, "Special Report: China's Gene Giant Harvests Data"; National Counter-intelligence and Security Center, "China's Collection of Genomic and other Healthcare Data from America."
[58] BGI Group, Annual Report 2020.
[59] BGI Group, "The NIFTY Test."
[60] Gadsbøll, "Current Use of Noninvasive Prenatal Testing in Europe, Australia and the USA."
[61] BGI Group, "The NIFTY Test."
[62] Bangkok Genomics, "Innovation."

Consent forms from 2022, suggest additional NIFTY testing labs may also be located in Hungary, Denmark, Australia, Uruguay and the United Kingdom.[63] The NIFTY tests use targeted genetic sequencing that examines specific mutations in a biological sample, and has been validated on around 150,000 pregnancies in China.[64] More than 12 million people worldwide had used the test by the end of 2022.[65]

While NIFTY tests that are ordered for foreign nationals may have their samples sent to BGI's laboratories in a third country for analysis, the genomic data come under the control of the company, and could potentially be transmitted anywhere it has offices, and to anyone they are obliged to share it with. Patients who use BGI's NIFTY test are required to consent to the storage and use of the remaining test material and associated data for the broad purpose of improving genetic diagnosis and treatment.[66] It has been reported that data from at least 500 women who have taken the NIFTY test, including women who did so outside of China, are stored in the China National GeneBank, a statement that BGI refutes: 'data collected from prenatal tests on women outside China are not stored in China's gene bank'.[67]

BGI's privacy policy explicitly states that genomic data can be shared when directly relevant to national security, public security, public health or significant public interest, opening a range of lawful possibilities for BGI to reuse biological samples and genomic data.[68] In 2021, BGI stated that the company 'has never been asked to provide, nor has it provided data from its NIFTY test to Chinese authorities for national security purposes'.[69] This would be difficult to verify, as all national security and defence-related requests for data sharing would be classified and could not be disclosed to the public.

Access to genomic data does not necessarily convert to applying that data: 'a number of bottlenecks and errors that can get introduced from the moment that a piece of biomedical big data is created through the journey to processing, storing, transferring, and using the data'.[70] National security and intelligence concerns relate to the vulnerability of biomedical databases to hacking, the possible creation of bioweapons and more general privacy and economic risks.[71] These should be sufficient context for law- and policy-makers to introduce mitigating regulatory reforms in relation to genomic data. Further, as noted above and discussed in greater detail in other articles, greater regulation of the commercial genomics sector in the United States requires further regulation to address issues such as privacy and data security.[72]

5. Addressing Genomic Security Concerns

5.1 Security Assessment

Genomic data regulation in the United States includes privacy, discrimination and data protection.[73] United States' intelligence assessments have consistently ranked Chinese access to and ownership of Americans' genomic data as a potential threat to national security. The four primary areas of concern include information security, data access and control, transfer of genetic data to foreign intelligence, military, and security agencies, and strategic economic competition.[74]

Genomic data can inform the related issue of genome editing, first publicly identified as a national security threat in 2016 in the annual report of the Office of the Director of National Intelligence: 'Research in genome editing conducted by countries with different regulatory or ethical standards than those of Western countries probably increases the risk of the creation of potentially harmful biological agents or products.'[75] Seven years on, and following the COVID-19 pandemic, assessments more clearly link genomic security with the national security of the United States. A more recent ODNI threat assessment acknowledges developments in genomic technologies as having the potential to both create scientific breakthroughs, but also to 'lead to the rapid development of asymmetric threats to U.S. interests'.[76] The potential for genomics to contribute to

[63] BGI Group, "Non-Invasive Prenatal Screening Test Request Form."
[64] Zhao, "Non-Invasive Prenatal Testing for Trisomies 21, 18 and 13."
[65] Needham, "Special Report: China's Gene Giant Harvests Data."
[66] BGI Group, "The NIFTY Test."
[67] Needham, "Special Report: China's Gene Giant Harvests Data."
[68] BGI Group, "Terms of Use and Privacy Policy."
[69] BGI Group, Annual Report 2020.
[70] Vogel, "Anticipating Emerging Biotechnology Threats."
[71] Office of the Director of National Intelligence, Worldwide Threat Assessment, 2022.
[72] Smith, "A Principled Approach to Cross-Sector Genomic Data Access"; Miller and Smith, "Quasi Universal Forensic DNA Databases."
[73] Arias, "The Growth and Gaps of Genetic Data Sharing Policies in the United States."
[74] Office of the Director of National Intelligence, Worldwide Threat Assessment, 2022.
[75] Coats, "Worldwide Threat Assessment of the US Intelligence Community."
[76] Office of the Director of National Intelligence, Worldwide Threat Assessment, 2022.

biological weapons that intelligence communities are not prepared to detect, attribute and treat is now a concern, and this would be closely associated with access to genomic data. Alongside Russia and Iran, China is identified as a non-allied country investing heavily in biosecurity. The security concerns raised by genomics that have been heightened by the China-based ownership of BGI include information security, data access and control and potential transfer to China's intelligence, military and security agencies for purposes contrary to the interests of the United States. The intelligence community and law-makers also consider China's genomic datasets a strategic threat in terms of technological advancements and economic competition.[77] During the COVID-19 pandemic, BGI contacted several US states and offered to provide COVID-19 testing kits and diagnostic services. US intelligence agencies sought to prevent states from taking up this offer on the basis that Americans' personal data may be acquired by China.[78]

The National Counterintelligence and Security Center (NCSC) has specifically identified Chinese-headquartered genomic companies as potential threats. In an unclassified report published in early 2021, NCSC wrote frankly about its overall understanding of China's collection of genomic and other data from the United States:

> Would you want your DNA or other healthcare data going to an authoritarian regime with a record of exploiting DNA for repression and surveillance? The PRC's collection of healthcare data from America poses … serious risks, not only to the privacy of Americans, but also to the economic and national security of the U.S.[79]

The NCSC's evaluation of the genomics industry in China considers the development priority that China's government has placed on advancements in this field, including nominating it as a 'strategic emerging industry' and prioritizing national support towards the industry in plans such as 'Made in China 2025'.[80] NCSC's evaluation also emphasizes its view that China-based actors have acquired genomic data from the United States both by legal and illegal means, such as a cybersecurity hacking.[81] Chinese companies have an obligation to work with intelligence agencies, including providing foreign and Chinese domestic genomic data to the state.[82]

Due to these privacy and data security concerns, the US Department of Commerce has added three companies from the BGI group – BGI Research, BGI Tech Solutions and Forensic Genomics International – to its Entity List of concern on the basis of a 'significant risk of contributing to monitoring and surveillance by the government of China'. It considers that they 'present a significant risk of diversion to China's military programs'.[83] This limits their access to sensitive technology developed by US companies. BGI Research, the largest offspring company in the list, issued a formal statement contesting involvement with the Chinese military, stating it is 'puzzled and greatly regret[s]' the decision and calling for 'further communication and verification' regarding the reasons for its inclusion.[84]

The 2019 Annual Report to Congress by the United States–China Economic and Security Review Commission identified that investment and cooperation in the US biotechnology sector provides Chinese corporations with access to vast volumes of US medical and genetic data, but no reciprocal access is provided to US enterprises; access to such data would now be restricted. BGI is the third largest DNA sequencing company worldwide, behind US companies Illumina and Thermo Fisher.[85] Business opportunities for companies in the sequencing business, such as genomic sequencing software or hardware, are likely to be affected significantly by inclusion in the Entity List. In the mid-year investor report in June 2023, BGI acknowledged three 'trade risks' associated with the listing: risk to international sales, international technology imports and supply chain disruptions.[86] The addition of BGI to the Entity List has been viewed in China as an anti-competitive move by the United States.[87]

5.2 Potential Regulation

While the United States has been more proactive in making its security assessments public regarding the threat posed by genomic data, related regulatory developments in Australia, which is aligned in terms of its national security policies, provide

[77] Office of the Director of National Intelligence, Worldwide Threat Assessment, 2023.
[78] Myre, "China Wants Your Data."
[79] National Counter-Intelligence and Security Center, "China's Collection of Genomic and Other Healthcare Data."
[80] National Counter-Intelligence and Security Center, "China's Collection of Genomic and Other Healthcare Data."
[81] National Counter-Intelligence and Security Center, "China's Collection of Genomic and Other Healthcare Data."
[82] Abelson, "Anthem Hacking Points to Security Vulnerability of Health Care Industry."
[83] Federal Register of the United States, "Additions and Revisions of Entities to the Entity List."
[84] BGI Group, Mid-Year Financial Report 2023.
[85] US–China Economic and Security Review Commission, Report to Congress.
[86] BGI Group, "Initial Public Offering and Listing on the GEM Prospectus."
[87] IVD Information, "Why Does the United States Always Shame BGI?"

insights into how it could potentially be addressed. In Australia, BGI has several approvals from the Therapeutic Goods Administration, including tests for COVID-19 and influenza, and is not subject to any listing or similar restriction.[88] Regulatory approaches could be developed in response to this issue, such as preventing foreign companies of potential concern, such as BGI, from providing services to Australian citizens on national security grounds. This would reflect recent approaches from the Australian Government in relation to Chinese companies in other sectors, where national security concerns have been raised. Indeed, comparisons have been made with the security threats posed by Huawei in relation to 5G communications technology and intelligence collection: 'BGI may be serving, wittingly or unwittingly, as a global collection mechanism for … sensitive personal information about key individuals around the world.'[89] The utilization of the genomics services provided by BGI present similar national security and regulatory issues as the potential collection of data via communication infrastructure in light of the Chinese National Intelligence Law. In fact, it is arguable that genomic data could be even more sensitive than telecommunications content.

As has occurred in relation to the use of Chinese technology in other contexts, the Australian Government could make a determination that Australian citizens cannot use the services of Chinese genomics companies or use their products where there is an attendant risk of data transfer (e.g. medical tests and associated equipment). This would follow the reasoning of the decision of the Australian National Security Committee of Cabinet in 2018 in relation to infrastructure for Australia's 5G network, on the basis that BGI would likely be 'subject to extra judicial directions from a foreign government that conflict with Australian law'.[90] In the Huawei case, the decision was made on the advice of the Australian Signals Directorate that allowing a Chinese company to provide such fundamental technology infrastructure would be too great a security risk. In the case of BGI, this could also be on the advice of national security and federal health agencies, and based on the fundamental importance of citizens' genomic data. Such an approach would accord with growing calls for a greater role of national security agencies in relation to health security now that the security implications of the COVID-19 pandemic are well understood, and gene editing technologies such as CRISPR have become available.[91]

Privacy compliance is important in the context of the issues discussed throughout the article, due to it providing a fundamental protection of personal data. Updated privacy and data-protection laws in relation to genomic data should be considered; however, these may be ineffective if the data are held offshore, and outside the jurisdiction, and more direct methods may be required. These approaches could be applied to genomic data across the board, not just in relation to foreign adversaries such as China.

There are already some legal protections of genomic data under Australian legislation, recognizing that the information is sensitive, and that it conveys health and other details about an individual, and potentially their family members. It is categorized as sensitive information under the *Privacy Act* and Privacy Principles.[92] Genomic information can only be disclosed where 'the organization reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the first individual'.[93] Legislation also makes it illegal to discriminate against a person on the basis of their genomic predisposition to a characteristic or disease, such as in employment contexts.[94]

If an Australian citizen purchases a genomic test from an overseas company, there is a question of whether that company could be subject to Australian law. In late 2022, new privacy legislation was passed.[95] Its extraterritoriality provisions remove the previous requirement that a company must collect or hold personal information in Australia in order to be subject to Australian law. Following this reform, a foreign company that is carrying on commercial activity in Australia will be subject to the *Privacy Act*, regardless of where the data are stored. The new legislation has also substantially increased the penalty for data breaches, now in the order of A$50 million, following several high-profile data breach cases in Australia during 2022. The federal government has stated that it wants to emphasize to companies their 'obligation to protect Australians' personal data, not to treat it as a commercial asset'.[96]

These regulatory developments, directed primarily at online platforms, make it more likely that overseas technology companies that do business in Australia, but hold Australians' data offshore, will be held accountable. This could also be applied to the

[88] BGI Group, Mid-Year Financial Report.
[89] National Security Commission on Artificial Intelligence, Annual Report, 53.
[90] Hartcher, "Huawei? No way!"
[91] Smith, "Improving Health Security and Intelligence Capabilities."
[92] *Privacy Act 1988* (Cth) s 4.
[93] *Privacy Act 1988* (Cth) s 16B(4).
[94] *Disability Discrimination Act 1992* (Cth), s 46(1)(f)–(g).
[95] *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Cth)
[96] *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Cth).

genomics sector and become a new governance model in this context. As the country's Attorney-General has stated, 'The novel privacy challenges posed by the rise of digital platforms and the unprecedented volume and variety of data that these platforms collect from users, underscores the importance of reforming our privacy laws.'[97] Enforcing such a law will be challenging, but it could place the actions of genomics companies under greater scrutiny, and result in improved data security. It could also be accompanied by a programme of education to inform Australians about genomic data protection, including that when they consent to a company using their data for research or law enforcement purposes, there may be implications for their relatives, and that the use of their data by multinational companies may not be regulated by Australian law.

There is wide variation around the world in the regulatory approaches in relation to genomic databases. Even in developed countries such as Australia and the United States, the framework is outdated and reforms are needed. Genomic data analytics and machine learning are rapidly growing fields, there is a vast and expanding amount of data available and growing security, economic, health and policy motives exist for it to be utilized. In addition to the security issues that must be addressed, reforms in this area could also help to deal with broader concerns about privacy rights, discrimination, ownership and data integration.

6. Conclusion

Developments in the field of commercial genomic technology provide insights into aspects of international security and technology regulation that are important and under-recognized in the literature, especially in light of the post COVID geopolitical environment. This article has argued that, as is occurring in relation to a number of areas of new technology, the actions of private genomics companies highlight a lack of regulation that is not only a risk to citizens' privacy, but can also threaten national security.

Ensuring that privacy regulation is fit for purpose can help to ameliorate the problem, but excluding a specific company, or country of origin of a specific product, may be necessary. We argue that it is appropriate for countries to prevent their citizens from using the services of particular foreign companies on security grounds. New regulation is urgently needed as potential end uses and associated security implications of genomic data will continue to evolve alongside continued scientific advancement. It is a key national resource, and greater attention should be directed to its security.

[97] Dreyfus, "International Association of Privacy Professionals Australia and New Zealand Summit 2022."

Bibliography

Abelson, Reed and Matthew Goldstein. "Anthem Hacking Points to Security Vulnerability of Health Care Industry." *New York Times*, February 5, 2015. https://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html.

Arias, Jalayne, Genevieve Pham-Kanter and Eric Campbell. "The Growth and Gaps of Genetic Data Sharing Policies in the United States." *Journal of Law and Bioscience* 2, no 1 (2015): 56–68. https://doi.org/10.1093/jlb/lsu032.

Australian Academy of Science (AAS). "Genome Sequencing COVID-19." 2021. https://www.science.org.au/news-and-events/events/genome-sequencing-covid-19.

Australian Strategic Policy Institute (ASPI). "Mapping China's Tech Giants." 2019. https://chinatechmap.aspi.org.au/#/homepage.

Bangkok Genomics. "Innovation." 2023. https://www.bangkokgenomics.com/wp-content/uploads/2018/11/NIFTY-Full-Request-Form.pdf.

BGI Group. "Initial Public Offering and Listing on the GEM Prospectus." 2017. https://archive.org/details/2017_20230822.

BGI Group. *Annual Report 2020*. 2021. http://www.szse.cn/disclosure/listed/bulletinDetail/index.html?b15cab91-ee0f-40df-bad2-3befca34d782.

BGI Group. "Non-Invasive Prenatal Screening Test Request Form." 2022. https://www.gravidklinikken.dk/wp-content/uploads/2023/01/NIFTY-Test-Request-Form-and-Inform-Consent.pdf.

BGI Group. "The NIFTY Test." 2023.https://www.bgi.com/global/service/the-nifty-test-non-invasive-prenatal-testing.

BGI Group. "Terms of Use and Privacy Policy." 2023. https://www.bgi.com/us/resources/privacy-policy.

BGI Group. *Mid-Year Financial Report*. 2023. https://archive.org/details/2017_20230822.

Bernot, Ausma and Marcus Smith. "Understanding the risks of China-made CCTV surveillance cameras in Australia." *Australian Journal of International Affairs* 77, no 4 (2023): 380–398. https://doi.org/10.1080/10357718.2023.2248915.

Bowman, Diana and David Studdert. "Newborn Screening Cards: A Legal Quagmire." *Medical Journal of Australia* 194, no 6 (2011): 319–322. https://doi.org/10.5694/j.1326-5377.2011.tb02985.x.

Capps, Benjamin, Ruth Chadwick, Yann Joly, Tamra Lysaght, Catherine Mills, John J. Mulvihill and Hub Zwart. "Statement on Bioinformatics and Capturing the Benefits of Genome Sequencing for Society." *Human Genomics* 13 (2019): Art. 24. https://doi.org/10.1186/s40246-019-0208-4.

Cave, Danielle, Elsa Kania, Tom Uren, Fergus Hanson, Peter Jennings, Michael Shoebridge, Jessica Clarence and Greg Austin. "Huawei and Australia's 5G Network." Australian Strategic Policy Institute, October 10, 2018. https://www.aspi.org.au/report/huawei-and-australias-5g-network.

China National Defense Science and Technology Information Center (CNDSTIC). "The Full Text of the '13th Five-Year Plan' Special Plan for the Development of Military-Civilian Integration of Science and Technology." October 27, 2017. http://www.aisixiang.com/data/106161.html.

China.org.cn. "China's First Gene Bank to Open in Shenzhen." 2016. http://www.china.org.cn/china/2016-09/21/content_39339851.htm

Coats, Daniel. "Worldwide Threat Assessment of the US Intelligence Community." May 1, 2017. https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf

Dencik, Lina and Jonathan Cable. "The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks." *International Journal of Communication* 11 (2017): 763–781. http://ijoc.org/index.php/ijoc/article/view/5524/1939.

Depoux, Dennis. "Can Chinese Giants Become Multinational Companies?" in *Transition and Opportunity. China and Globalization*, edited by H. Wang and L. Miao, 147–158. New York: Springer, 2022.

Dreyfus, Mark. "International Association of Privacy Professionals Australia and New Zealand Summit 2022." November 23, 2022. https://ministers.ag.gov.au/media-centre/speeches/international-association-privacy-professionals-australia-and-new-zealand-summit-2022-23-11-2022.

Federal Register of the United States. "Additions and Revisions of Entities to the Entity List." June 3, 2023. https://www.federalregister.gov/documents/2023/03/06/2023-04558/additions-and-revisions-of-entities-to-the-entity-list.

Feero, Gregory, Catherine Wicklund and David Veenstra. "Precision Medicine, Genome Sequencing, and Improved Population Health." *Journal of the American Medical Association* 319, no 19 (2018): 1979–1980. https://doi.org/10.1001/jama.2018.2925.

Ferguson, Victor and Darren Lim. "Economic Power and Vulnerability in Sino-Australian Relations." In Jane Golley, Linda Jaivin and Sharon Strange (eds), *China Story Yearbook: Crisis*, 259–274. Canberra: ANU Press, 2021.

Gadsbøll, Kasper, Olav B. Petersen, Vincent Gatinois, Heather Strange, Bo Jacobsson, Ronald Wapner, Joris R. Vermeesch, The NIPT-map Study Group and Ida Vogel. "Current Use of Noninvasive Prenatal Testing in Europe, Australia and the USA: A Graphical Presentation." *Acta Obstetricia et Gynecologica Scandinavica*. 99, no 6 (2020): 722–730. https://doi.org/10.1111/aogs.13841.

Girard, Bonnie. "The Real Danger of China's National Intelligence Law." *The Diplomat*, February 23, 2019.

Golley, Jane, Amanda Barry, Paul Harris and Darren J. Lim. "Geoeconomics and the Australian University Sector: A 'Geoeducation' Analysis." *Security Challenges* 16, no 4 (2020): 24–40.
Hartcher, Peter. "Huawei? No Way! Why Australia Banned the World's Biggest Telecoms Firm." *Sydney Morning Herald*, May 21, 2021. https://www.smh.com.au/national/huawei-no-way-why-australia-banned-the-world-s-biggest-telecoms-firm-20210503-p57oc9.html.
Huada Genomics. "From Technological Innovation to Internationalisation Upgrade: Creating a Sample of Precision Medicine Industry." April 12, 2023. https://archive.md/9LGAx.
Illumina. "Illumina Files Patent Infringement Suit Against BGI in Germany." 2019. https://sapac.illumina.com/company/news-center/press-releases/2019/2392777.html.
IVD Information. "Why Does the United States Always Shame BGI?" 2023. https://archive.md/wip/PQ6xl.
Kania, Elsa and Wilson VornDick. "China's Military Biotech Frontier: CRISPR, Military–Civil Fusion, and the New Revolution in Military Affairs." *China Brief* 19, no 18 (2019). https://jamestown.org/program/chinas-military-biotech-frontier-crispr-military-civil-fusion-and-the-new-revolution-in-military-affairs.
Li, Zhenzhen, Zhang Jiuchun, Wen Ke, Hall Thorsteinsdottir, Uyen Quach, Peter A. Singer and Abdallah S. Daar. "Health Biotechnology in China: Reawakening of a Giant." *National Biotechnology* 22, no 12 (2004): DC13–DC18. https://doi.org/10.1038/nbt1204supp-dc13.
Lynch, David. "MPs Call for Probe into Chinese Genetics Company Over Pregnancy Test Data." May 23, 2023. https://www.independent.co.uk/news/uk/alistair-carmichael-chinese-ico-mps-henry-smith-b2344208.html.
Miller, Seumas and Marcus Smith. "Quasi Universal Forensic DNA Databases." *Criminal Justice Ethics* 41, no 3 (2022): 238–256. https://doi.org/10.1080/0731129X.2022.2141021.
Mittal, Akshay. "Digital Health: Data Privacy and Security with Cloud Computing." *Issues in Information Systems* 2221, no 1 (2020): 227–238.
Myre, Greg. "China Wants Your Data – and May Already Have It." NPR, February 24, 2021. https://www.npr.org/2021/02/24/969532277/china-wants-your-data-and-may-already-have-it.
The National Counter-intelligence and Security Center (NCSC). "China's Collection of Genomic and other Healthcare Data from America: Risks to Privacy and U.S. Economic and National Security." 2021. https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf.
National Development and Reform Commission of the People's Republic of China. "The 13th Five-year Plan for Economic and Social Development of the PRC." 2021. https://en.ndrc.gov.cn/policies/202105/P020210527785800103339.pdf.
National Security Commission on Artificial Intelligence (NSCAI). *Annual Report.* 2021. https://www.nscai.gov/2021-final-report.
Needham, Kirsty and Clare Baldwin. "Special Report: China's Gene Giant Harvests Data from Millions of Women." July 7, 2021. https://www.reuters.com/article/us-health-china-bgi-dna-idUSKCN2ED1A6.
Oliveira, Arlindo. "Biotechnology, Big Data and Artificial Intelligence." *Biotechnology Journal* 14, no 8 (2019): 1–6. https://doi.org/10.1002/biot.201800613.
Office of the Director of National Intelligence. *Worldwide Threat Assessment.* February 2022. https://www.odni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.
Office of the Director of National Intelligence. 2023. *Worldwide Threat Assessment*. February 2023. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.
Parliament of Australia. "Select Committee on Foreign Interference Through Social Media." September 25, 2020.
Pearson, Margaret, Meg Rithmire and Kellee Tsai. "China's Party-State Capitalism and International Backlash: From Interdependence to Insecurity." *International Security* 47, no 2 (2022): 135–176. https://doi.org/10.1162/isec_a_00447.
Qiang, Xiao. "The Road to Digital Unfreedom: President Xi's Surveillance State." *Journal of Democracy* 30, no 1 (2019): 53–67. https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-president-xis-surveillance-state.
Regalado, Antonio. "More Than 26 Million People Have Taken an At-Home Ancestry Test." *MIT Technology Review*, 11 February 2019. https://www.technologyreview.com/2019/02/11/103446/more-than-26-million-people-have-taken-an-at-home-ancestry-test.
Regalado, Antonio. "China's BGI Says It Can Sequence a Genome for just $100." *MIT Technology Review*. February 26, 2020. https://www.technologyreview.com/2020/02/26/905658/china-bgi-100-dollar-genome.
Simon, Tobby. "Critical Infrastructure and the Internet of Things." In *Global Commission on Internet Governance: Cyber Security in a Volatile World*. Washington, DC: Centre for International Governance Innovation and the Royal Institute of International Affairs, 2017.
Satam, Heena et al. "Next-generation Sequencing Technology: Current Trends and Advancements." *Biology* 12, no 7 (2023): 997. https://doi.org/10.3390/biology12070997.
Smith, Marcus and Patrick Walsh. "Improving Health Security and Intelligence Capabilities to Mitigate Biological Threats." *International Journal of Intelligence, Security, and Public Affairs* 23, no 2 (2021): 139–155. https://doi.org/10.1080/23800992.2021.1953826.

Smith, Marcus. *DNA Evidence in the Australian Legal System*. Sydney LexisNexis, 2016.
Smith, Marcus and Gregor Urbas. *Technology Law: Australian and International Perspectives*. Cambridge: Cambridge University Press, 2021.
Smith, Marcus and Seumas Miller. "A Principled Approach to Cross-Sector Genomic Data Access." *Bioethics* 35, no 8 (2021): 779–786. https://doi.org/10.1111/bioe.12919.
US–China Economic and Security Review Commission. Report to Congress. November 2019. https://www.uscc.gov/sites/default/files/2019-11/2019%20Annual%20Report%20to%20Congress.pdf.
Vogel, Kathleen and Sonia Ouagrham-Gormley. "Anticipating Emerging Biotechnology Threats: A Case Study of CRISPR." *Politics and Life Science* 37, no 2 (2018): 203–209. https://doi.org/10.1017/pls.2018.21.
Vogel, Kathleen and Sonia Ouagrham-Gormley. "China's Biomedical Data Hacking Threat: Applying Big Data Isn't as Easy as it Seems." *Texas National Security Review* 5, no 3 (2022): 2576–1153. http://dx.doi.org/10.26153/tsw/42078.
Wan, Zhiyu, James W Hazel, Ellen Wright Clayton, Yevgeniy Vorobeychik, Murat Kantarcioglu and Bradley A. Malin. "Sociotechnical Safeguards for Genomic Data Privacy." *National Reviews Genetics* 23 (2022): 429–445. https://doi.org/10.1038/s41576-022-00455-y.
Wang, Kai, Xiaobai Shen and Robin Williams. "Sequencing BGI: The Evolution of Expertise and Research Organisation in the World's Leading Gene Sequencing Facility." *New Genetics and Society* 40, no 3 (2021): 305–330. https://doi.org/10.1080/14636778.2020.1843148.
Wang, Ruiyan, Qin Cao, Qiuwei Zhao and Yin Li. "Bioindustry in China: An Overview and Perspective." *New Biotechnology* 40 (2018): 46–51. https://doi.org/10.1016/j.nbt.2017.08.002.
Wang, Sarah. "Big Pharma Would Like Your DNA." *The Atlantic*, July 27, 2018.
Wei, Liping and Jun Yu. "Bioinformatics in China: A Personal Perspective." *Plops Computational Biology* 4, no 4 (2008): e1000020. https://doi.org/10.1371/journal.pcbi.1000020.
Wong, Terry. "Characterizing the Harms of Compromised Genetic Information for Article III Standing in Data Breach Litigation." *Columbia Journal of Law and Social Problems* 53, no 4 (2020): 461–508.
World Health Organization (WHO). "Human Genomics in Global Health." 2020. https://www.who.int/genomics/geneticsVSgenomics/en
Xia, Christine and Ajay Gautam. "Biopharma CRO Industry in China: Landscape and Opportunities." *Drug Discovery Today* 20, no 7 (2015): 794–798. https://doi.org/10.1016/j.drudis.2015.02.007.
Yasiejko, Christopher. "Illumina, BGI Group Units Settle U.S. Suits on DNA-Sequencing Tech." July 16, 2023. https://news.bloomberglaw.com/ip-law/illumina-bgi-group-units-settle-us-suits-on-dna-sequencing-tech.
Zhang, Joy and Saheli Burton. 2022. *The Elephant and the Dragon in Contemporary Life Sciences: A Call for Decolonising Global Governance*. Manchester: Manchester University Press.
Zhang, Pan and Zhuoling Liao. "Behind the Rising Influence of Chinese Research." *Elsevier Connect*, 27 June 2022. https://www.elsevier.com/connect/behind-the-rising-influence-of-chinese-research.
Zhao, Hongyun et al. "Non-Invasive Prenatal Testing for Trisomies 21, 18 and 13: Clinical Experience from 146 958 Pregnancies." *Ultrasound in Obstetrics and Gynaecology* 45, no 5 (2015):–538. https://doi.org/10.1002/uog.14792.

Legislation cited

Disability Discrimination Act 1992 (Cth), s 46(1)(f)–(g).
Privacy Act 1988 (Cth) s 4.
Privacy Act 1988 (Cth) s 16B(4).
Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 (Cth)
Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 (Cth).