Internet 2.0 submission to the Select Committee on Foreign Interference through Social Media

16 Feb 2023

By:

David Robinson

Chair & Co-Chief Executive Officer, Internet 2.0

Strategic Intelligence Advisor to CI-ISAC

Retired Australian Army Intelligence Officer

Level 1, 18 National Circuit, Barton, ACT, 2600, Australia
ABN: 17 632 726 946 (Internet 2.0 Pty Ltd)

Contents

Summary

This submission has been submitted by Internet 2.0 to the Select Committee on Foreign Interference through Social Media. It is the primarily the opinions of the Author and Co-CEO Robert Potter.

In summary, our philosophical position is that risks to serious national security should be placed ahead of offering free market principles to social media corporations that reside in, originate from, or are leveraged by authoritarian regimes. The data created by social media companies are a finite and valuable asset that is on the frontline of the strategic competition between liberal democracies and authoritarian regimes. Possession of this data allows informational advantage within this strategic competition, especially if used by artificial intelligence and other sophisticated software and intelligence platforms. Social Media companies are the primary producer of this data and social media corporations that reside in, originate from, or are leveraged by authoritarian regimes cannot defend themselves against sophisticated intelligence collection.

If a social media platform must balance the competing needs of both liberal democracies and authoritarian regimes, we are accepting risk to the integrity of our future elections in democracy. The integrity of our social media platforms is now a pillar of democratic elections and must be defended. If we allow authoritarian regimes unfettered access to our social media platforms, we accept serious ongoing risk – given we assess influence and disinformation campaigns against elections will increase.

Finally, because of artificial intelligence we assess time is not on our side to make decisions about these complex policy issues. Artificial intelligence is increasing the effectiveness of influence and disinformation campaigns against elections. When combined with high quality data, we cannot guarantee we can defend ourselves and we will not be able to reverse the loss of trust our system will suffer.

We implore the Parliament to take sound and bipartisan action to defend our citizens' data against its collection by authoritarian regimes; reduce the risk of digital foreign influence by limiting the access of social media corporations that are leveraged by authoritarian regimes; and regulate the use of artificial intelligence in the media, journalism, and election information.

Underlying Philosophy of our argument

Internet 2.0 needs to outline our philosophical approach and position to this entire topic before going into the technical details of our argument. We do this because we believe members of parliament philosophically must decide on their approach before they dive into the technical policy decisions. The hypothetical question we pose to outline our philosophical position to this topic is:

When dealing with how to strengthen Australians in cyber security and privacy provisions, as well as mitigate the risks of foreign interference through digital avenues, does the voting member weigh national security above free market principles or vice versa?

In the course of undertaking to debate this topic, we ask that members make clear their position – particularly with respect to where free market principles should come before national security. In our assessment, liberal democracies afford free market principles to companies which ultimately reside in authoritarian countries, sometimes at our own detriment, because these economic principles are so valuable that we must uphold them as an extension of our liberal democracy. Taking this opinion is

the philosophical counter argument to our position which is existential threats to national security must come before offering free market principles to corporations run from authoritarian regimes.

Our position, that existential threats to national security must come before offering free market principles to corporations run from authoritarian regimes, actually aligns with our adversaries' viewpoint as well. Our authoritarian competitors already have made the decision to limit social media access for their residents because digital access is a national security threat for them as well. By their nature, authoritarian regimes see the security of their regime to be paramount above all. Take, for example, China's Great Firewall, and the many western social media companies which are banned from operating in China – uncensored information is an existential risk to their power. In 2022, Russia removed the ability for people without a Russian phone number to create an account on VKontakte, effectively limiting its usage to the borders of Putin's regime.

We believe that the benefits of free market principles should not be extended to companies that reside in authoritarian regimes. They should not be allowed to gain profit and capital at the expense of our national security. Ultimately, they do not reside in our society. Social media companies that reside in our society will contribute and attempt to uphold democratic values. These companies should be defended against social media companies that align with our authoritarian competitors, because they flourish only as a result of our free-market principles and democratic system.

Why data is central to this debate

In our assessment, possession of high quality social, psychological, political, military, and economic data is a frontline in the strategic competition between authoritarian states and liberal democracies. This is because the internet and social media has changed key features of the information domain in this strategic competition.

Our ability to process large amounts of data and derive strategic and tactical insights quickly is enabled by the current capabilities of social media, machine learning, and computing. The primary resource to make these insights is high quality data produced by social media companies. These social media companies originally produce it to create advertising revenue. In and of itself, this would be an economic benefit, however – in our assessment – authoritarian states have co-opted it to gain an advantage in information dominance within the strategic competition.

For China big data is one of their stated primary fields for strategic competition. In 2015 China's State Council released its data strategy titled "Outline of Action for Promoting the Development of Big Data". China's data strategy sees it as a new opportunity to reshape its competitive advantage.

> *"Big data has become a new opportunity to reshape the country's competitive advantage… Make full use of my country's data scale advantage….enhance the ability to protect cyberspace data sovereignty, and maintain national security. Effectively enhance the national competitiveness….Build a big data industry ecosystem with multiparty linkage and coordinated development of government, industry, academia, and research."*[1]

In China's Thirteenth Five-Year Plan for National Economic and Social Development of the People's Republic of China [Chapter 27] Implementing the National Big Data Strategy, China proposed to invest heavily in data collection and analysis.

[1]http://www.gov.cn/zhengce/content/2015-09/05/content_10137.htm

"Deepen the innovative application of big data in various industries, explore the coordinated development of new business forms and new models with traditional industries, and accelerate the improvement of the big data industry chain. Accelerate key technological breakthroughs in the fields of massive data collection, storage, cleaning, analysis and exploration, visualization, security and privacy protection. "[2]

China has a culture of using the "thousand grains of sand" concept to build its national competitiveness in big data. In 2018 Willian Evanina, the US Director of the National Counterintelligence and Security Center 2014- 2021, stated:

"China is devoting "ungodly resources" and increasingly employing "more aggressive" and "more diversified" non-traditional means to conduct espionage against the United States. It's a persistent thousand grains of sand. They hit our academia, our industry, our research development, and obviously our government"[3]

We can only see the symptoms of these strategic programs, which limits our insight into what strategic data capability our authoritarian competitors possess. Examples such as the Zhenhua Data leak, published by Internet 2.0 in September of 2022, which had data on the top 35,000 Australians, was a window to this build up of strategic competition.[4] The Zhenhua Database was made up primarily of social media data built upon the foundation of a hacked anti money laundering database. It was designed to give social, economic, and psychological insights onto the global cadre of leaders who contribute to the architecture of national decision making, and was tailored to focus specifically on military and political targets in the United States – despite its global coverage. Internet 2.0 released key facts and outlined our assessment of the Zhenhua Data Platform; Figure 1 is a graphic which displays how combining multiple datasets across sectors gave the Zhenhua database broad coverage and the opportunity to gain information dominance.

Figure 1. Zhenhua Data Overview

[2] http://www.xinhuanet.com//politics/2016lh/2016-03/17/c_1118366322.htm
[3] https://www.cbsnews.com/news/ncsc-director-says-china-is-the-largest-threat-to-national-security/
[4] https://www.afr.com/policy/foreign-affairs/china-s-social-media-warfare-database-lists-key-australians-20200910-p55u95

As covered in the Australian Financial review, in response to the Zhenhua Data leak, Matthew Pottinger, the Deputy National Security Adviser to President Donald Trump, called out China's digital surveillance campaign and its efforts to "intimidate", "blackmail", and "influence" foreign citizens. He said assembling such "dossiers" had always been part of Leninist regimes and their efforts to influence, humiliate, divide, and blackmail opponents, while noting this had become far easier in the digital age.[5] We must also note that this type of platform, in our opinion, cannot be built in a liberal democracy with intelligence oversight. Western Intelligence laws are underpinned by the belief of collecting only information that is required in a value of proportionality, which also is a value under the international laws of armed conflict.

As possession of high quality social, psychological, political, military, and economic data is a key resource in gaining advantage in the information domain, our question – as it relates to foreign interference through digital means – is whether social media companies which reside in or is leveraged by authoritarian regimes have the sophistication to balance the interests of both their authoritarian regimes and our government. Given we are in strategic competition, are we willing to offer free market principles in the hope these companies can balance our values of privacy and proportionality?

In our assessment, authoritarian regimes have already breached these values of privacy and proportionality. They know the value of the data, and have moved to collect it on us and limit our access to it in their social media domain. They also conduct mass surveillance through social media within their own borders. We have demonstrated this through their use of database platforms in China in the Shanghai files leak.[6]

Under these conditions, because they build their own applications with surveillance in mind, there is no culture of building mobile software applications with privacy in mind.[7] When they export these business models to our social media environments the legacy of this surveillance culture permeates. TikTok has serious flaws in terms of security and privacy. When rated against all other social media applications, their android app rated double the average on a security and privacy framework.[8] The application closest to TikTok was VK, followed Didi. It is an alarming trend that the outliers on the bell curve are all Russian and Chinese applications which are exported to our markets. We doubt any of these applications could stop a sophisticated intelligence operation if an authoritarian regime was given an opportunity to collect data.

As social media companies are the primary producer of high quality social, psychological, political, military, and economic data, liberal democracies must move to defend this data by limiting the access to it by authoritarian regimes. This should be implemented in both a software application regulatory policy and a wider data regulatory policy. In our view, the commercial access points to buy this data are as big a threat as the hacking of this data.

[5] https://www.afr.com/policy/foreign-affairs/white-house-china-s-digital-dossiers-to-blackmail-and-intimidate-20201025-p568c7
[6] https://www.abc.net.au/news/2021-04-01/shanghai-files-shed-light-on-china-surveillance-state/100040896
[7] https://internet2-0.com/whitepaper/digital-surveillance-in-china/
[8] https://internet2-0.com/whitepaper/its-their-word-against-their-source-code-tiktok-report/ https://blog.malcore.io/p/tiktok-scores-631-designed-to-collect

Elections

Our authoritarian competitors hold the view that our elections are a strategic opportunity to influence our democratic process. They believe that it is to their benefit if the voting population have less confidence in the true results of elections. By conducting divisive campaigns, they seek to divide our societies, to weaken us, and to fracture our uniting values. Effective disinformation campaigns that target elections rely on social media companies having no stake in upholding democratic values. Regardless of the deemed effectiveness of the actions by social media companies, in their attempt to label or remove disinformation, it is still at least an attempt to uphold democratic values and defend against disinformation. We assess that social media companies which reside in our authoritarian competitors' orbit will not act in our democratic interests; if we attempt to compel them to remove disinformation, they can resist this as they balance the competing interests of the authoritarian regime. They can resist our sovereign interventions by hosting data, media, and their platforms outside of our jurisdiction. WeChat poses this risk as all of their news and public social media data is managed from their Hong Kong Gateway that interfaces with their China mainland network.[9] The fundamentally globalised nature of the internet, in this case, is our weakness. Their access to our information environments through social media is a strategic risk, as their ability to mount an effective disinformation campaign against our elections relies on this access.

Effective disinformation campaigns also rely on high quality data to have insight into voting patterns. Cambridge Analytica is an example of what the Zhenhua Data example can evolve into. Key themes and messages disinformation campaign push must be sophisticated to be effective. In the case of Cambridge Analytica high quality social data was critical. Botnets are also already deployed on behalf of authoritarian regimes. Internet 2.0 published the paper "Influence Botnets: 2021 Myanmar Coup"[10] which showed the sophisticated Russian Botnet Platform SANA attacking the Pentagon's social Media accounts on 16 to 17 February 2021 to conduct disinformation in the United States immediately following the 2021 Coup in Myanmar.

Future Risk

Artificial intelligence increases the existential risks outlined in our position. Artificial intelligence will enable disinformation campaigns as it exponentially increases the computation and distribution of high quality information. Journalism is a key measure we use to defend against foreign interference through social media. The implications of artificial intelligence, if it is not regulated in its use within journalism, elections, and the media, are that our authoritarian adversaries will have the advantage in the information domain. If they still have access to our social media domain in a meaningful way, with the growing capability of artificial intelligence we will increasingly be placing our system of government at great risk. We believe that before artificial intelligence becomes mainstream in social media, it must be regulated, and that authoritarian regimes' access to our social media and data must be cut off.

[9] https://internet2-0.com/whitepaper/wechat-analysis/
[10] https://internet2-0.com/whitepaper/influence-bots/

Annexes

Internet 2.0 has released multiple public papers and investigative stories that provide a lot of context to our position and are referenced in this document. To save our submission length we refer members to the public reports enclosed.

Annex A Zhenhua Data Leak

Annex B Influence Botnets: 2021 Myanmar Coup

Annex C TikTok Report

Annex D Mobile App Industry Survey

Annex E Chinese Olympics Mobile Applications

Annex F WeChat Report