Data Can be Dangerous, but US, Canadian, and German Officials See Different Risks in Data Troves

Introduction

Americans, Canadians and Germans have seen first-hand that the online world is simultaneously a wondrous and dangerous place. They rely on computer and mobile phone applications that collect personal data. However, Americans, Canadians, and Germans have also learned that when they give personal information to private firms, that data can be misused, stolen, and hacked, creating a plethora of security risks. Data troves can be crossed to identify individuals, putting personal security at risk. As these threats become more common and severe, national security is also at risk ((Cyberspace Solarium Commission 2020, 93).

Herein we define *national security* as policies to maintain the legitimacy and survival of the state. Security threats can include warfare, terrorism, cyber-threats, and contagious diseases (AAAS, FBI and UNICRI 2014). We define *personal data* as data by and about people (WEF: 2011, 5) and *data troves* as large pools of allegedly anonymized person data.

This paper attempts to examine how personal data held by private firms became a national security problem in the United States and compares the US response to that of Canada and Germany. Citizens in all three countries give personal information to many of the same data giant firms. Policymakers and scholars in all three nations have warned of potential national security spillovers of large data troves. However, Canadian and German officials are more focused on the infrastructure where data is stored and processed. They want to ensure that Canadian and German laws apply to Canadian and German personal and/or government data when it is stored on the cloud.

This paper is organized as follows. We first show that although adversaries have long used personal data to gain an advantage, policy makers began to identify troves of personal data as a national security risk around 2012. We then discusses the relationship between personal data governance and security in the United States. We then focus on specific cases. We then examine how the Trump Administration responded to this dilemma and compare it to the data and national security threat envisioned by German and Canadian policy makers. Finally, we present conclusions.

Methodology

We use qualitative case studies and process tracing (a technique to examine causal mechanisms and how they change over time) to better understand and compare how the three governments see the national security risk inherent in data troves. The cases provide a "most different" design, whereby there is considerable variation across internet application (e.g. photo app, video app, social network etc.), countries affected, variance in laws providing protection of data, and alleged effects on national security).

The cases provide examples of the complex interactions between data providers (netizens) and data companies. The cases include both social networks and apps. Social networks are websites or applications where people can meet, collaborate, share and stay in touch. They are built on free data provided by users, which is then sold to other firms such as advertisers and data brokers.. Apps are small programs that increase the functionality of a service, as example, they can make texting easier, direct individuals to voting sites, or help put users to sleep. App firms often use personal data to create new products and services, but they also often sell large troves of anonymized personal data to other firms. Although apps and social networks are different, social networks are often available in app format-e.g. the Strava app.[1] Both make money from personalized ads.

We do not contend that these four cases present a representative sample. These cases do not include financial, retailing, or goods-producing firms, which also collect and monetize a lot of data, nor do these cases include data brokers such as Experian, which buy and sell personal data. Moreover, the four cases are not equally popular in all the countries although with the exception of Totok, the apps were generally present in the main app stores.[2]The four cases have one thing in common: a US government official or agency asserted that the app or social network presented a national security risk.

The cases illuminate how troves of data can make individuals and/or nations vulnerable by reducing their control over personal data. As example, many apps allow advertisers to access phone or computer functions (such as location data or contact lists) that are not essential for the app to operate (Betts et al: 2013). A 2019 study of apps in India found that more than 95 percent of available mobile apps and websites in India share or sell data toh third parties without the user's permission (Arkka 2019, 8, 10). Although app stores often require app firms to certify they only access certain functions, they rarely enforce their

[1] https://actonline.org/wp-content/uploads/Deloitte-The-App-Economy-in-US.pdf, 3–5, 17).

[2] We reviewed each of the apps popularity at various points in time on the Google play and Apple App stores through ranking services such as app annie, https://www.appannie.com/en/ and similar web https://www.similarweb.com/ Among the 4, Totok was the only one not present in top 500 rankings in the 3 countries.

own rules. In so doing, they put their clients' personal security at risk (Austin et al: 2018).

When large troves of data are hacked or crossed, national security can be threatened. However, nations are not equally vulnerable by these threats because they have different levels and approaches to protecting personal data(Cobb: 2018, Abrahams: 2019). Although the United States lacks a national personal data protection law, it has strong protections for personal data in sectoral laws and robust enforcement tools. Germany has strong national and EU data protections, but so far has not been able to ensure that firms with large data troves adequately protect that data.[3] Meanwhile, Canada has a strong personal data protection law, but relatively weak tools of enforcement (OPC: 2019).

TABLE 1 HERE

Literature Review

Data and national security have a complex relationship. Data is essential to national security-it can help defense officials understand and counter adversaries. Moreover, large troves of various types of data underpin many modern military tools such as drones or artificial intelligence. Finally, governments collect lots of data about their citizens. Reliance on that data could lead to national security vulnerabilities, because government data sets are vulnerable to theft, hacking, and misuse (Van Puyvelde et al: 2017)

However, the private sector today controls the bulk of personal data. In the early years of the web, most companies providing web applications such as browsers and social networks adopted a business model where if netizens provided personal data, they could receive these services for free. Firms would then utilize that data to better understand customers, solve problems and create new goods and services. But soon users became the product, as these firms also used this data to predict and shape human behavior. Scholar Shoshana Zuboff described this as 'surveillance capitalism' (Zuboff: 2019) Users had no leverage to stop these firms from this use of their data without direct consent (On Point: 2019; Hartzog:2018). Meanwhile, economists noted that companies that build up large datasets have an incentive to hoard and not share this data, stifling competition and reducing the potential benefits of

[3] https://iapp.org/resources/article/the-general-data-protection-regulation-matchup-series/; https://iapp.org/resources/article/gdpr-at-one-year-dpas/; www.dlapiperdataprotection.com/index.html?c=DE&c2=US&go-button=GO&t=law, comparing the United States and Germany; and www.dlapiperdataprotection.com/index.html?c=CA&c2=US&go-button=GO&t=law. On Office of the Privacy Commissioner of Canada (OPC), see OPC (2019).

data. Moreover, because data markets are opaque, neither governments or users know if companies are doing enough to protect the data they hold from theft and misuse (Carrière-Swallow and Haksar 2019).

Still other scholars and activists asserted that as data became the key input into new digital goods and services, these services began to undermine human rights, autonomy, trust, and democratic stability (Betts et al: 2013; Lipman: 2016 Privacy International: 2007; Amnesty International: 2019.) The Office of the High Commissioner for Human Rights asked a Special Rapporteur to detail the dangers of surveillance capitalism. (Office of the High Commissioner for Human Rights: 2019) Citizen Lab , a Canadian research lab focused on digital threats,[4] concluded that companies that collect vast amounts of user data, such as apps and fitness trackers, will become attractive targets for government agencies and criminal organizations. Some governments may compel companies to turn over user data, making these companies "proxies" for state surveillance and espionage (Scott-Railton and Hilton 2018).

Meanwhile, scholars began to show that when personal data is collected in bulk and then anonymized, it can easily be de-anonymized by crossing multiple data sets (Ohm 2010; Campbell-Dollaghan 2018). Since nation states are comprised of people, nation states are also vulnerable. For example, in 2019, *The New York Times* reported that even US President Donald Trump could be tracked using cellphone data from his Secret Service agents and/or those individuals who meet with him. "Foreign actors like Russia, North Korea, China and other adversaries may be working to steal, buy or otherwise obtain this kind of data" (Thompson and Warzel 2019).

Scientific and US government agencies began to recognize that these huge troves of data could have negative effects not just on individuals but on national security. In 2012, the US General Accounting Office (GAO) found that when firms collect and share location data, consumers could be subject to increased surveillance, higher risk of identity theft, or threats to personal safety (GAO 2012).

In 2013, the Department of Defense's research arm (DARPA) funded a study examining if " the availability of data provide a determined adversary with the tools necessary to inflict nation-state level damage" (Neal: 2013). The results were not made public. In 2014, the American Association for the Advancement of Science (AAAS), recommended that the US government develop "security strategies that can be integrated in an open source environment where large datasets are collected, aggregated, and analyzed" (AAAS, FBI and UNICRI 2014, 13; In 2015, the National Academy of Sciences wrote a similar analysis for the

[4] https://citizenlab.ca/category/research/app-privacy-and-security/

intelligence community (National Academy: 2015). In 2019, the Director of National Intelligence warned that in America's data-intensive economy, citizens won't feel secure if the personal data is inadequately protected. (Coates: 2019). Meanwhile GAO warned that the US Government has not adequately focused on how the collection and use of consumers' personal information, such as their internet browsing histories, purchases, locations etc. might affect national security (GAO 2019). Despite these multiple warnings from governmental and scientific bodies, data troves did not become a policy issue until policymakers saw China's increased interest in acquiring personal data as well as Chinese excellence in new data-driven sectors from e-commerce to apps.

Despite this history, we could find no scholarly study of how these troves might threaten national security or compared national responses. However, several journalists and researchers have examined this issue (Cordero 2018; Biancotti 2019; Albrycht 2020; Thompson and Warzell 2019) This study builds on their work, examining both the alleged threats and government responses.

How did the Treat Posed by Inadequate Governance of Personal Data Arise?

Individuals have long used personal information to manipulate others. However, because so many firms seek and inadequately protect personal data, the problem has become more daunting and pervasive. Several recent factors explain this development.

- **Transition to a data-driven economy**: Many middle-income and wealthy countries are transitioning toward economies built around the collection, protection, and understanding of many different types of data (World Economic Forum 2011).
- **Rising demand for data sets:** Researchers, officials and firms using new technologies such as AI or data analytics need large and often multiple troves of data to solve complex problems. As the demand and supply of data rises, the potential for hacking, theft, misinformation and other problems also increases.
- **Massive increase in data volume**: The largest data firms such as Google, Facebook and Apple[5] collect and store extensive data about their users (Amnesty 2019). But they are not alone; almost every service provider and store seek to collect, analyze and use customer data. Meanwhile, the number of connected devices is exploding. The European Commission estimates that the volume of global data is expected to grow from 33

[5] Google stores an individual's search history across all of their devices, information on every app and extension they use, and all of their YouTube history, while Facebook collects data about people even if they do not have a Facebook account.

zettabytes in 2018 to 175 zettabytes in 2025 (European Commission 2020). A zettabyte is 1,000,000,000,000,000,000,000 bytes.

- **Rise of tracking**: Web advertisers want to track where users go. Ghostery, a browser extension designed to protect user privacy, studied 850,000 users from 12 countries in 2017 and found that at least one tracker was prowling around 77.4 percent of the tested page loads for those users (Ghostery 2017). In 2018, *The New York Times* reported that at least 75 companies receive anonymous, precise location data from mobile apps.[6]
- **Inadequate governance of data markets**: The market for personal data is global, essentially underregulated and opaque. Consequently, users do not know about price, demand, supply, buyers and/or sellers (Aaronson 2018).
- **Difficulty protecting large troves of data from threats, including theft, manipulation, data loss and so forth**: In 2018, Dell Technologies surveyed a wide range of private and public organizations around the world and found they manage 13.53 petabytes on average, a whopping 831 percent increase since 2016.[7]
- **A plethora of bad actors in cyberspace:** Authoritarian governments, hackers and criminals can steal and manipulate data and hide from the law.[8]
- **Data is easy to exploit**: For example, during the 2016 US presidential election, Russian operatives purchased stolen US identities, opened US bank and PayPal accounts, and purchased Facebook ads and "buttons, flags, and banners" for political rallies. These operatives also employed virtual private networks to pose as Americans on US social media accounts. (Landau 2018).
- **Openness to foreign investment may create additional vulnerabilities:** Most industrialized countries such as the United States, Canada and Germany are relatively open to foreign investment.[9] Adversaries can take advantage of this openness and use front companies, joint ventures, mergers and acquisitions, and direct investment to gain access to firms with data troves (Office of the Director of National Intelligence 2020).

How Did Troves of Personal Data Become a National Security Issue in the United States?

[6] www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[7] See www.delltechnologies.com/content/dam/uwaem/production-design-assets/en/gdpi/assets/infographics/dell-gdpi-vb-key-findings-deck.pdf, slides 1–3, 10, 21, 34, 35). Dell updated the study in 2020, see www.delltechnologies.com/en-us/data-protection/gdpi/index.htm#gdpi_2020.

[8] See www.nsa.gov/what-we-do/understanding-the-threat/.

[9] See www.law360.com/corporate/articles/1212390/security-fears-dog-doj-as-foreign-tech-cos-collect-us-data.

In 2013, the US government admitted that it had not adequately protected the personal data of many federal workers. Hackers breached the US Office of Personnel Management (OPM), where they stole personnel records from more than 21 million current and former federal government employees and contractors.[10] Although Beijing denied involvement, the US government concluded that China was behind the OPM hack and could combine this official data with other data sets.[11] With such data mixing, China could use various analytics techniques to predict or better understand US policies and actions.

Meanwhile, US policy makers also discovered that adversaries could monitor and target individual members of US military online. In 2014, *The New York Times* reported that a group linked to the Islamic State of Iraq and Syria (ISIS), released a "hit list" containing the personal information of 100 current and former American military service members. In response, officials from the Federal Bureau of Investigation (FBI) and the Department of Homeland Security urged members of the military to scrub their social media accounts.[12] In 2015, US Central Command warned its soldiers, "Don't share your usernames, passwords, or network details. ..Listing your hobbies, likes, dislikes, etc., could be useful information to an enemy, especially for gaining trust and rapport before seeking other information."[13] Despite this warning, ISIS again targeted members of the US military in Kuwait in 2020.[14]

During the Obama administration (2009–2016), officials began to fear that China, an authoritarian state, was gaining an information tech advantage, which it could use for military advantage and to repress human rights (Sacks 2020). Under the protection of the Great Firewall, Chinese companies had developed a wide range of innovative data-driven services from messaging, to scooter and ride rental, to sophisticated data analysis, threatening the lead of the West (Aaronson and Leblond 2019). China exceled at stealing intellectual property from firms and appeared to be using similar strategies to steal personal data from both government and private sector firms. According to Aspen Institute Scholar Garrett Graff, "Chinese intelligence has amassed in just five years a

[10] See www.nextgov.com/cybersecurity/2015/06/timeline-what-we-know-about-opm-breach/115603/.
[11] See www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html, and www.washingtonpost.com/opinions/2019/04/09/why-we-cant-leave-grindr-under-chinese-control/.
[12] See https://identity.utexas.edu/id-perspectives/isis-targeting-military-members-via-social-media.
[13] See www.centcom.mil/VISITORS-AND-PERSONNEL/SOCIAL-MEDIA-SECURITY/; www.oge.gov/web/oge.nsf/0/16D5B5EB7E5DE11A85257E96005FBF13/$FILE/LA-15-03-2.pdf.
[14] See www.militarytimes.com/flashpoints/2020/01/15/family-members-of-deployed-paratroopers-receiving-menacing-messages-warned-to-double-check-social-media-settings/.

database more detailed than any nation has ever possessed about one of its adversaries. The data …work both to identify existing US intelligence officers through their personnel records and travel patterns as well as to identify potential weaknesses — through background checks, credit scores, and health records — of intelligence targets China may someday hope to recruit" (Graff 2020). The US Department of Justice launched the "China Initiative" in November 2018, with the aim of countering Chinese national security threats, including trade secret and IP theft, hacking and economic espionage.[15]

Although the US was probably the first nation to view data troves as a national security problem, it has lagged in developing effective national legislation to protect that data. As the cases below illuminate, netizens of the United States have little recourse to ensure that their personal data does not put them or their fellow Americans at risk.

The Cases

Case 1 – An Indirect Insider Threat: Strava's Use of Geolocation and Personal Fitness Devices and Its Impact on National Security

Strava is one of the world's most popular social networks for athletes.[16] Individuals use Strava to record their activities and can compete against others for time or distance. In November 2017, several engineers at Strava created and posted a heat map (a data visualization) of all of its users' training data in 2017 (Robb 2017).[17] The heat map showed where and how far Strava users ran, walked, swam or biked between 2015 and September 2017. The data was anonymized, global and huge — it included 700 million activities culled from the app's approximately 27 million users (Robb 2017; Sly 2018).

In January 2018, Nathan Ruser, then a grad student in Australia, reviewed the map and took to Twitter to publicize his concerns. He noted that "US bases are clearly identifiable and mappable." (He also pointed out Russian and Turkish military activity, and others followed on Twitter with their own analysis.)[18] Some tweets described potential drone locations and alleged CIA black sites.[19]

According to *Wired*, other researchers soon cross-referenced Strava user activity with Google Maps and prior news reporting to find hidden French and Italian military bases in Africa. In fact, the Strava heat map seemed to reveal several

[15] See www.cnbc.com/2019/09/23/chinese-theft-of-trade-secrets-is-on-the-rise-us-doj-warns.html.
[16] As of February 2020, Strava claimed some 50 million users. https://blog.strava.com/press/strava-milestones-50-million-athletes-and-3-billion-activity-uploads/
[17] https://www.strava.com/heatmap#4.89/-127.17403/40.99786/hot/all
[18] Ruser's tweet and the responses can be found at https://twitter.com/Nrg8000/status/957318498102865920.
[19] See https://twitter.com/AlecMuffett/status/957615895899238401.

Western military and civilian operations in developing countries. It also could be used to identify individuals by mixing the heat-map data set with other data source. (Hsu 2018). A scholar at the Monterey Institute asserted that anyone with access to the data could make a pattern of life maps for individual users, some of whom may be very interesting to foreign intelligence services. (Lewis 2018).

The US military and many of its allies responded immediately to these revelations about the heat map. *The Washington Post* reported that the US-led coalition against the said it would revise its guidelines on the use of all wireless and technological devices:" (Sly 2018). In August 2018, the Pentagon announced that all active-duty Department of Defense personnel would be prohibited from using tracking functions on their phones and devices in operational areas (any place where the military is conducting a specific mission). Commanders can allow use on a case-by-case basis only after doing a security survey.[20]

The author could find no information as to whether the Canadian or German military altered their practices in the wake of the Strava heat-map revelations. But the United States is not alone in viewing apps or social networks that provide location data as a potential threat to national security. Interestingly, the Chinese government banned its military personnel from using wearables on duty in 2015, in recognition that these devices might inadvertently reveal information on its activities (Sonnad 2015).

Case 2 – An Outsider Threat: FaceApp (Allegedly Affiliated with the Russian Government)

Many people like to use their phones to take self-portraits, or "selfies." In 2017, a new app promised users it could make it easier to perfect or improve these pictures. FaceApp allows its users to change their gender, hair, and age. The company uses AI to "transform your photos or videos into works of art or change the background or foreground, overlay objects with different objects and clone/copy the style or effects from other image or video."[21]

By 2019, more than 100 million users downloaded the app on Google Play alone.[22] In June, *The Washington Post* noted that because the app became popular so quickly, some feared that it might be a disinformation campaign

[20] See https://media.defense.gov/2018/Aug/06/2001951064/-1/-1/1/GEOLOCATION-DEVICES-APPLICATIONS-SERVICES.PDF.

[21] See www.faceapp.com/terms-20170803.html.

[22] https://www.forbes.com/sites/johnkoetsier/2019/07/17/viral-app-faceapp-now-owns-access-to-more-than-150-million-peoples-faces-and-names/#6ab145b662f1

(Fowler 2019). The Democratic National Committee warned individuals to delete the app (Denham and Harwell 2019).

FaceApp seems designed to give the company a lot of information from users' phones. Under the app's terms of service, "You grant FaceApp a perpetual, irrevocable, nonexclusive, royalty-free, worldwide, fully-paid, transferable sub-licensable license to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, publicly perform and display your User Content and any name, username or likeness provided in connection with your User Content in all media formats and channels now known or later developed, without compensation to you."[23] The company can then use the data it collects for its own purposes.

The CEO of FaceApp, Yaroslav Goncharov, stated that FaceApp deletes "most" of the photos from its servers after 48 hours. The company also asserted that it does not store user data on Russian servers (Fowler 2019). However, soon thereafter, the company tightened its terms of service, but analysts still viewed the app as a privacy risk. If a user deletes content from the app, under its terms of service, FaceApp can still store and use it. FaceApp also says it cannot guarantee that users' data or information is secure, and that the company can share user information with other companies and third-party advertisers, which is not disclosed in the privacy terms (Denham and Harwell 2019).

In July 2019, Senator Chuck Schumer noted the popularity of the app and asked the FBI to investigate if it was safe. In late November 2019, the FBI responded that it "considers any mobile application or similar product developed in Russia, such as FaceApp, to be a potential counterintelligence threat based on the data it collects, its privacy and terms of use, and the legal mechanisms available to the government of Russia that permit access to data within Russia's borders."[24]

The FBI;s analysis focused on the outside threat rather than America's failure to enact clear personal data protection rules. In addition, the United States has no rules governing app permissions, relying on Apple, Android, Amazon and other platforms to govern their app stores. Canada and Germany also rely on platforms to set and enforce the rules for app behavior and use of personal data. However, as of this writing, neither Canada nor Germany identified FaceApp or similar applications as a national security threat.

[23] See www.faceapp.com/terms-20170803.html.

[24] See www.democrats.senate.gov/imo/media/doc/FBI%20Letter%20to%20Schumer%20re%20FaceApp11.pdf.

Case 3 – An Outsider Threat: ToTok (An App Used by the United Arab Emirates to Spy on Its Citizens:

ToTok[25] (not to be confused with TikTok, discussed later) is a free messaging and calling app. It was one of the top free apps in Saudi Arabia, Britain, India, Sweden and a number of other countries, although it was not among the top 500 in the United States, Germany or Canada. In some countries in the Middle East, ToTok was one of the few apps that was not subject to a ban (Cherian 2020). The app may have been designed to spy on its users, yet it is still available at many app stores.

Apple, Google, Microsoft, Garmin and other companies with such stores derive many benefits from them. They can build trust and gain valuable information about the applications that their users download and utilize. To be approved for sale or use, app store companies such as the firms noted above require that apps must pass a broad test for safety; provide a detailed privacy policy; and disclose what data it collects, how it uses personal data and how long it is retained.[26] Nonetheless, developers can code malicious intent into their applications and evade the companies' rules (Newcombe 2019).

ToTok presented a new challenge to app stores. In a December 2019 report, *The New York Times* used background information from classified briefings for US intelligence officials and its own analysis to show that the messaging app ToTok was created and used by the UAE government as a surveillance tool. The *Times* reported that it did not know whether US officials have confronted their counterparts in the UAE government about the app, although the authors believe the United States has warned some governments (Mazetti et al. 2019).

The app appears to be a form of spyware that can be used to monitor text and chat messages; record phone logs; track social media posts; log website visits; activate microphones, cameras and GPS systems; register keystrokes and block calls. Governments and/or individuals that use spyware can control and repress another individual, undermining their rights and autonomy (Parsons et al. 2019). Security expert Patrick Wardle confirmed that the iOS-version of ToTok did collect users' entire address book and upload it to ToTok servers (Goodin: 2020).

The *Times* reported that the app was re-engineered from a free Chinese messaging app, Yee Call, which offered free video calls. The app was then re-engineered by Pax AI, an Abu Dhabi-based data mining firm that is linked to

[25] https://totok.ai/

[26] For Apple's guidelines, see https://developer.apple.com/app-store/review/guidelines/#legal. For Google's policies, see https://play.google.com/about/developer-content-policy/.

another Abu Dhabi-based cyber-intelligence and hacking firm called Dark Matter.[27] The firm allegedly customized the app to meet the needs of the UAE government through the addition of spyware (Mazzetti, Perlroth and Bergman 2019). The United Arab Emirates has long relied on private firms to build its intelligence capacity (McLaughlin 2017).

In response to the allegation, the company's founder argued, "Since day one, we have built ToTok with user security and privacy as our priority."[28] The company also claimed that the reason ToTok was allowed to operate in the United Arab Emirates (while other messaging apps such as FaceTime, WhatsApp, and Skype are not available in the country) was because the app started as a pilot project that had met all the United Arab Emirates' regulatory requirements." (Warwick 2019). Some companies banned the app. As of February 2020, the app was not available on Google's or Apple's app store, but it was ed available for download on the company web site as well as on Samsung, Huawei and other app stores (Goodin: 2020). The author could find no information that other nations had banned ToTok, although the app seemed to violate app store guidelines.

Meanwhile, as of May 2020, the US government has not publicly warned users about ToTok nor stated publicly that a foreign government created it. But if these allegations are true, they reveal how difficult it is to protect users from enticing apps designed to obtain large pools of personal data.[29]

Case 5 – TikTok: An Outsider Threat and a Threat to Free Speech?

TikTok is one of the world's most popular apps for making and sharing short videos. As of May 2020, the app has been downloaded more than 2 billion times, with over 800 million active users.[30]

TikTok's parent company, ByteDance, describes its business as producing AI. As users watch videos, the app uses AI to learn what users look for, and then it makes suggestions. But to some observers, the app looks like an enticing strategy to build a pool of personal data from users. In fact, Byte Dance was fined by the US Federal Trade Commission (FTC) in February 2019 because it found the company did not obtain parental consent before collecting children's personal data (Herrman 2019). Moreover, in May 2020, some 20 civil society organizations claimed that the firm continued to violate US privacy regulations.

[27] See www.helsinkitimes.fi/finland/finland-news/domestic/16165-revealed-secretive-uae-cybersecurity-firm-with-a-history-of-spying-on-dissidents-is-operating-in-finland.html.
[28] See https://totok.ai/news-dec24.
[29] Research have found bogus COVID-19 apps deployed in Armenia, Brazil, India, Colombia, Indonesia, Iran, Italy, Kyrgystan, Russia and Singapore that steal personal data. https://www.enca.com/news/researchers-say-bogus-contact-tracing-apps-deployed-steal-data
[30] https://techcrunch.com/2020/04/29/tiktok-tops-2-billion-downloads/

As of May 2020, UK and Dutch investigators are also examining whether the firm breached privacy laws (Bergman, Frenkel and Zhong 2020 and Murphy: 2020).

In September 2019, *The Guardian* obtained leaked documents that purportedly showed TikTok instructing its moderators to censor videos that mentioned topics sensitive to the Communist Party of China such as Tiananmen Square, Tibetan independence and Falun Gong. *The Guardian*'s investigation came after *The Washington Post* noted that a search for Hong Kong-related topics on TikTok showed virtually zero content about the pro-democracy protests (Bergman, Frenkel and Zhong 2020). But it also came at a time when US companies and officials such as Senators Hawley, Cotton, and Schumer expressed concern about foreign (read Chinese) competition in data-driven services (Smith 2019). In congressional testimony, Matt Perault, then Facebook's head of global public policy,[31] testified that the company felt challenged by TikTok (Overly 2019).

But Tiktok is extremely popular in the US. The US Army Recruiting Command used the app to recruit soldiers and surpassed its 2019 recruiting goal (Cox 2019a).

In October 2019, a bipartisan group of senators asked US intelligence officials to investigate whether TikTok represents a national security risk to the United States (Cox 2019a; 2019b). The company responded to allegations that it censors and does not protect data, noting that its "user data is stored and processed in the U.S. and other markets where TikTok operates at industry-leading third-party data centers. It's important to clarify that TikTok does not operate in China and that the government of the People's Republic of China has no access to TikTok users' data" (Caroll 2019).

Meanwhile, an arm of the US Treasury Department, the Committee on Foreign Investment in the United States (CFIUS), began to examine how the company purchased a US video platform to build the TikTok platform and whether such ownership constituted a threat to US security (Alexander 2019; Cox: 2019a; 2019b). Senator Schumer told *The New York Times* on November 1, 2019, that the security review is a "validation of our concern that apps like TikTok — that store massive amounts of personal data accessible to foreign governments — may pose serious risks to millions of Americans" (Schumer 2019; Nicas et al. 2019).

One month later, in December 2019, the Department of Defense sent out a cyber awareness message identifying "TikTok as having potential security risks associated with its use." The guidance directs all Defense Department

[31] See https://sanford.duke.edu/articles/former-facebook-global-policy-expert-lead-tech-policy-initiative-duke.

employees to "uninstall TikTok to circumvent any exposure of personal information." Meanwhile, the service cannot ban personnel from using TikTok on their personal phones, but Army leaders recommend that service members use caution (Cox 2019b). In March 2020, several senators proposed a bill to ban US government employees from downloading and/or using TikTok on government devices.[32]

In January 2020, Check Point Research, an Israeli cyber security firm, discovered multiple vulnerabilities within the TikTok application. These vulnerabilities allowed attackers to obtain TikTok accounts and manipulate their content, delete videos, make private "hidden" videos public and reveal personal information (Boxiner et al. 2020).

TikTok's rapid growth threatened the market leadership of US entertainment/video apps. But was it really a security threat? TikTok was clearly using its AI expertise to entice users and could then utilize their personal information to build or sell to other businesses. Quartz's David Carroll researched the company's privacy policies and found that user data could be shared "with any member or affiliate of [its] group" in China. TikTok later confirmed that "data from TikTok users who joined the service before February 2019 may have been processed in China," and possibly shared with Chinese government entities (Carroll 2019). On March 16, 2020, TikTok announced that it would carefully monitor the platform for disinformation and would do so from the United States (Wall Street Journal 2020). In May 2020, the newspaper USA Today examined the company's practices and concluded it is no more prone to hacking than other social media platforms.[33]

The United States stands alone in its concerns about the app. While other countries such as the United Kingdom have investigated the company, Germany and Canada (and other governments) have not banned its use.

Comparing US, German and Canadian Policy Responses to the Threat of Data Troves

In 2018, the Trump administration and members of Congress began to acknowledge that they needed a broader approach to addressing potential national security spillovers related to big data troves. But they did not focus on strengthening personal data protection, developing technical solutions to protect privacy, or devising strategies to ensure that anonymization was

[32] See S.3455 – No TikTok on Government Devices Act, a bill to prohibit certain individuals from downloading or using TikTok on any device issued by the United States or a government corporation (see www.congress.gov/bill/116th-congress/senate-bill/3455/text?q=%7B%22search%22%3A%5B%22TikTok%22%5D%7D&r=1&s=2).

[33] https://www.usatoday.com/story/news/factcheck/2020/05/18/fact-check-tiktok-security-threat-used-hackers-traffickers/3120617001/

effective, in particular when data sets are crossed. Instead, in August 2018, Congress passed and President Trump signed into law the Foreign Investment Risk Review Modernization Act (FIRRMA), which required that CFIUS review foreign investment in new technologies, national security-related infrastructure and other areas.[34] The law reflected congressional concerns that such transactions could "expose personally identifiable information, genetic information, or other sensitive data of U.S. citizens to access by a foreign government or person to exploit information to threaten national security" (Jackson and Cimino-Isaacs 2020).

In May 2019, President Trump issued an executive order that found that "the unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities…and thereby constitutes an…extraordinary threat to the national security…of the United States." The president then banned such transactions.[35] In short, despite its long history of openness to foreign investment, the United States would now carefully review foreign investment in firms with large holdings of data.

After seeking public comments, the Treasury Department issued final regulations that allowed CFIUS to review transactions where a firm could exploit personal data in a manner that threatens US national security.[36] The Treasury developed 10 categories of sensitive data including genetic, biometric and medical data and data pertaining to personal finance, communications and security clearances.[37]

The Trump Administration also warned about other services that are built on aggregated data. In 2019, the Pentagon asked military personnel to stop using at-home DNA kits for health and ancestry purposes, fearful that such data could be sold, hacked and crossed (Graff 2020).[38] Moreover, the United States rethought its counterintelligence strategy, recognizing that it must work with the private sector and research organizations to protect sensitive data (Office of the Director of National Intelligence 2020, iii). But Congress made little

[34] See www.treasury.gov/resource-center/international/Documents/Summary-of-FIRRMA.pdf.

[35] See www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

[36] The final regulations are available at https://s3.amazonaws.com/public-inspection.federalregister.gov/2020-00188.pdf.

[37] https://s3.amazonaws.com/public-inspection.federalregister.gov/2020-00188.pdf). The law made exemptions for investors from the United Kingdom, Canada and Australia because of the intelligence-sharing relationships among these countries.

[38] Interestingly, US intelligence agencies are trying to use such data (see www.axios.com/government-wants-access-to-personal-data-while-it-pushes-privacy-aacc15f1-bbcb-481b-b6ae-278e0f15e678.html).

progress on a national online personal data protection law, despite concerns about personal data protection related to the pandemic of 2020.

Meanwhile, Canadian and German officials are also concerned that troves of personal data could pose a national security threat if stolen or misused. But neither has enacted foreign investment restrictions or reviews of firms that seek to merge or acquire other firms with large troves of data. Both countries have restricted government officials from using Zoom for official meetings based on its failure to adopt end to end encryption, but they have not banned other apps for misuse of data.[39] Instead, they worry that Canadian and German firms do not own or control the cloud infrastructure where their data is stored and processed. Both nations are working to achieve "sovereignty" over data in the cloud.

To Canada, data sovereignty is based on the idea that certain types of data have a *national* "home" — a venue that data should reside in because it belongs to, and may hold information about, or is considered sensitive to that home. Governments have long had rules designed to govern the storage and transfer of sensitive data, such as military information. However, when that data is stored in the cloud, in servers located outside that country, the rules may be unclear.

In 2018, Canada established rules governing the use and storage of various types of data.[40] Non-Canadian cloud service providers can comply with these rules by storing data in Canada. However, the Treasury Board (which advises the government) noted, "Canada cannot ensure full sovereignty over its data when it stores data in the cloud. GC (government of Canada) data could be subject to foreign laws and be disclosed to another government. Under some foreign laws, disclosure of GC data could take place without notice to the GC." Thus, the Treasury Board recommended that the government limit the types of data stored in the commercial cloud.[41]

In 2019 Parliamentary testimony, Andrew Clement, professor emeritus at the University of Toronto, noted that at least 25 percent of all internet communications in Canada are routed through the United States. He

---

[39] On zoom, see for Canada https://www.cbc.ca/news/technology/taiwan-zoom-video-conference-1.5524384 and for Germany, see https://www.mobileworldlive.com/apps/news-apps/germany-bans-zoom-app-as-privacy-concerns-grow/

The author researched bans by examining cyber-security agencies in both countries (the Canadian Centre for Cyber Security and alerts and advisories and by doing a search of banned apps (see https://www.bsi.bund.de/EN/TheBSI/Functions/functions_node.htmlhttps://cyber.gc.ca/en/alerts-advisories

[40] See www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/direction-electronic-data-residency.html.

[41] See www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/gc-white-paper-data-sovereignty-public-cloud.html.

recommended that "all sensitive and critical Canadian domestic data be stored, routed and processed within Canada."[42] Influenced by his testimony, Parliament's Standing Committee on Public Safety proposed that Canada should "enhance its connectivity with Europe and Asia, while reducing its reliance on the United States."[43]

However, Canada has yet to announce a clear strategy to prevent national security risks from public or private personal data troves. In March 2020, Public Safety Canada prepared a briefing book for the minister of Public Safety Canada. The briefing book "identified four gateways which state and non-state actors are using to exploit Canadian technology and expertise, obtain personal data, and access critical infrastructure — all of which create economic-based threats to national security. These four gateways or threat vectors include – foreign investment, trade and exports, knowledge, as well as rights and licenses….Each continues to present unique threats." The rest of the memo was redacted, so it is unclear how Canada will proceed.[44]

While Canada is still evolving its approach to protecting data through assertion of data sovereignty, Germany is has long worked to achieve digital sovereignty. In 2017, the German Federal Office for Information Security announced that testing, using and providing open source software would preserve German sovereignty in the age of digitalization.[45] On October 29, 2019, German Chancellor Angela Merkel announced that the European Union should reclaim its "digital sovereignty" by developing its own platform to manage data and reduce its reliance on US data-driven firms (Chazen 2019). The German government explained that digital sovereignty is "the possibility of independent self-determination by the state and by organizations with regard to the use and structuring of digital systems themselves, the data produced and stored in them, and the processes depicted as a result."[46]

Germany and other nations have begun the "Gaia-X" project, which "aims at setting up a secure and trustworthy data infrastructure for Europe that meets the highest standards of digital sovereignty while promoting innovation. This project is the cradle of an open, transparent digital ecosystem, where data and services can be made available, collated and shared in an environment of

[42] House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Andrew Clement, professor emeritus, Faculty of Information, University of Toronto), 42nd Parliament, 1st Session, 18 March 2019.
[43] www.ourcommons.ca/Content/Committee/421/SECU/Reports/RP10589448/securp38/securp38-e.pdf, 42–46.
[44] www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/trnstn-bndrs/20191120/030/index-en.aspx.
[45] P. 7, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2017-02.pdf?__blob=publicationFile&v=2
[46] www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/das-projekt-gaia-x-executive-summary.pdf?__blob=publicationFile&v=6, 3.

trust."[47] Non-European companies can participate but must abide by European rules around data protection and "sovereignty," still to be defined.[48] As of June 2020, the project is establishing use cases.[49]

Findings

As this paper has illuminated, the United States, Canada and Germany see risk in huge troves of personal data held in the cloud, in apps or in social networks. The threat will only mount as more people are connected to devices and provide even more of their data.

However, the three nations have different definitions of the problem and adopted three different responses to the issue. US policy makers see a problem in the ownership and use of data. The United States has asked national security personnel to not use certain apps, asked the FBI to review national security risks, and adopted investment reviews of foreign firms that want to acquire firms with large troves of personal data. The US has acted as if this is a foreign policy problem rather than a domestic governance problem. Meanwhile, Canada and Germany are concerned about *where and how* data is stored and processed. They are determined to ensure that Canadian and German laws apply to Canadian and German personal and/or government data when it is stored on the cloud (often on US cloud service providers). Both nations fear that they are too reliant on US cloud infrastructure to store various types of data and they want this data to be governed under their laws.

The US approach, focusing on app bans and investment reviews, looks protectionist and can do little to build trust in US data-driven services. In fact, the US strategy looks more like a response to declining US market share and rising competition in the creation and provision of data-driven services. Meanwhile, the German and Canadian approaches also look increasingly protectionist with a focus on ensuring data sovereignty.

The case studies reveal that strong data protections may to some degree protect individuals, but these may need to be updated to meet the ever-evolving data economy. With apps and social networks, a few large firms act as gatekeepers and censors. Sometimes, as we may have seen with ToTok, dangerous applications slip through the cracks. App stores firms need to establish clearer policies and stronger enforcement strategies to prevent the

[47] *Ibid*. and https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html
[48] See https://fortune.com/2019/10/30/europe-cloud-independence-gaia-x-germany-france/?showAdminBar=true.
[49] See www.bmwi.de/Redaktion/EN/Artikel/Digital-World/data-infrastructure.html; and . https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

misuse of applications. As example, while it is appropriate for an app affiliated with a car company to gather data on how often a driver brakes, that app should not be seeking that driver's contact list or camera.

The case studies also reveal that even when governments see similar risks in data troves, they are not cooperating on policy solutions. Nations should make interoperable language for national laws protecting personal data a top priority. In addition, the United States, Canada and Germany should collaborate to define and mitigate the risks in privately held data troves, as example reporting on bogus apps and misuse of permissions. In so doing, we can collectively mitigate the dangers of aggregated data held by private firms.

References

AAAS, FBI and UNICRI. 2014. *National and Transnational Security Implications of Big Data in the Life Sciences*. www.aaas.org/sites/default/files/AAAS-FBI-UNICRI_Big_Data_Report_111014.pdf.

Aaronson, Susan Ariel. 2018. "Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows." CIGI Paper No. 197, November 14. Waterloo, ON: CIGI. www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows.

Aaronson, Susan Ariel and Patrick Leblond. 2018. "Another Digital Divide: The Rise of Data Realms and its Implications for the WTO." *Journal of International Economic Law* 21 (2): 245–72. doi:10.1093/jiel/jgy019.

Albrycht, Sarah. 2020. "When the Homefront becomes the (cyber) front line." Fifth Domain, February 3. www.fifthdomain.com/opinion/2020/02/03/when-the-homefront-becomes-the-cyber-front-line/.

Alexander, Julia. 2019. "TikTok owner ByteDance denies it's exploring selling stake in popular app." The Verge, December 24. www.theverge.com/2019/12/24/21036850/tiktok-bytedance-sale-stale-bloomberg-musically-congress-investigation-china.

Amnesty International. 2019. *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*. www.amnesty.org/en/documents/pol30/1404/2019/en/.

Arrka. 2019. *State of Data Privacy of Mobile Apps & Websites from India*. https://iapp.org/media/pdf/resource_center/state_privacy_apps_websites_india_2019.pdf.

Austin, Lisa M. and Lie, David and Sun, Peter and Spillette, Robin and D'Angelo, Mariana and Wong, Michelle, Towards Dynamic Transparency: The AppTrans (Transparency for Android Applications) Project (June 27, 2018). Available at SSRN: https://ssrn.com/abstract=3203601

Bergman, Ronen, Sheera Frenkel and Raymond Zhong. 2020. "Major TikTok Security Flaws Found." *The New York Times*, January 8. www.nytimes.com/2020/01/08/technology/tiktok-security-flaws.html.

Betts, Jennifer and Scott-Hayward, Sandra and Sezer, Sakir and Miller, Robert, Same Issues, New Devices: Is Smartphone App Privacy Groundhog Day for Regulators? (June 4, 2013). Available at SSRN: https://ssrn.com/abstract=2351189 or

BBC News. 2014. "Data protection: Angela Merkel proposes Europe network." BBC News, February 15. www.bbc.com/news/world-europe-26210053.

———. 2018. "Fitness app Strava lights up staff at military bases." BBC News, January 29. www.bbc.com/news/technology-42853072.

Biancotti, Claudia. 2019. "For the United States, More Digital Privacy Would Mean More National Security." Peterson Institute for International Economics, April 10. www.piie.com/blogs/realtime-economic-issues-watch/united-states-more-digital-privacy-would-mean-more-national.

Boxiner, Alon, Eran Vaknin, Alexey Volodin, Dikla Barda and Roman Zaikin. 2020. "Tik or Tok? Is TikTok secure enough?" Check Point Research, January 8. https://research.checkpoint.com/2020/tik-or-tok-is-tiktok-secure-enough/.

Campbell-Dollaghan, Kelsey. 2018. "Sorry, your data can still be identified even if it's anonymized." Fast Company, October 12. www.fastcompany.com/90278465/sorry-your-data-can-still-be-identified-even-its-anonymized.

Canadian Centre for Cyber Security. 2019. *2019 Update: Cyber Threats to Canada's Democratic Process*. https://cyber.gc.ca/en/guidance/executive-summary-1.

Carrière-Swallow, Yan and Vikram Haksar. 2019. "The Economics of Data." *IMF Blog* (blog), September 23. https://blogs.imf.org/2019/09/23/the-economics-of-data/?utm_medium=email&utm_source=govdelivery.

Carroll, David. 2019. "Is TikTok a Chinese Cambridge Analytica data bomb waiting to explode?" Quartz, May 7. https://qz.com/1613020/tiktok-might-be-a-chinese-cambridge-analytica-scale-privacy-threat/.

Chazan, Guy. 2019. “Angela Merkel urges EU to seize control of data from US tech titans.” *Financial Times*, February 12. www.ft.com/content/956ccaa6-0537-11ea-9afa-d9e2401fa7ca.

Cobb, Stephen. 2018. “Data Privacy vs. Data Protection: Reflecting on Privacy Day and GDPR.” WeLiveSecurity, January 25. www.welivesecurity.com/2018/01/25/data-privacy-vs-data-protection-gdpr/.

Cordero, Carrie. 2018. “Corporate Data Collection and U.S. National Security: Expanding the Conversation in an Era of Nation State Cyber Aggression.” *Lawfare* (blog), June 1. www.lawfareblog.com/corporate-data-collection-and-us-national-security-expanding-conversation-era-nation-state-cyber.

Cox, Matthew. 2019a. “Army Recruiters Still Using TikTok Amid National Security Probe.” Military.com, November 7. www.military.com/daily-news/2019/11/07/armyden-recruiters-still-using-tiktok-amid-national-security-probe.html.

Cox, Matthew. 2019b. “Army Follows Pentagon Guidance, Bans Chinese-Owned TikTok App.” Military.com, December 20. www.military.com/daily-news/2019/12/30/army-follows-pentagon-guidance-bans-chinese-owned-tiktok-app.html.

Cyberspace Solarium Commission. 2020. *CSC Final Report*. March. www.solarium.gov/report.

Dalby, Beth. 2019. “FaceApp: 5 Things To Know About Privacy And National Security” Patch, July 22. https://patch.com/us/across-america/faceapp-5-things-know-privacy-national-security.

Dell Technologies. 2018. *Global Data Protection Index 2018*. www.delltechnologies.com/content/dam/uwaem/production-design-assets/en/gdpi/assets/infographics/dell-gdpi-vb-key-findings-deck.pdf.

Deloitte Japan. 2017. *Defense Policy and the Internet of Things: Disrupting Global Cyber Defenses*. www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-IoT-defense-policy-and-the-internet-of-things.pdf.

Denham, Hannah and Drew Harwell. 2019. “FaceApp went viral with age-defying photos. Now Democratic leaders are warning campaigns to delete the Russian-created app ‘immediately.’” *The Washington Post*, July 17. www.washingtonpost.com/technology/2019/07/17/faceapp-adds-decades-your-age-fun-popular-russian-owned-app-raises-privacy-concerns/.

European Commission. 2020. *The European Digital Strategy*. February. https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy.

Fowler, Geoffrey A. 2019. "You downloaded FaceApp. Here's what you've just done to your privacy." *The Washington Post*, July 17. www.washingtonpost.com/technology/2019/07/17/you-downloaded-faceapp-heres-what-youve-just-done-your-privacy/.

FTC. 2014. *Data Brokers: A Call for Transparency and Accountability*. May. www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

GAO. 2012. "Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy." GAO-12-903, October 11. www.gao.gov/products/GAO-12-903.

GAO. 2019. "Consumer Privacy: Changes to Legal Framework Needed to Address Gaps." GAO-19-621T, June 11. www.gao.gov/products/GAO-19-621T.

Ghostery Team. 2017. "Tracking the Trackers: Ghostery Study Reveals that 8 Out of 10 Websites Spy on You." December 4. www.ghostery.com/study/.

Gilbert, David. 2020. "Iran Launched an App That Claimed to Diagnose Coronavirus. Instead, It Collected Location Data on Millions of People." Vice News, March 14. www.vice.com/en_us/article/epgkmz/iran-launched-an-app-that-claimed-to-diagnose-coronavirus-instead-it-collected-location-data-on-millions-of-people.

Goodin, Dave, 2020. "The strange, unexplained journey of ToTok in Google Play fuels user suspicions," Ars Technica, February 21, https://arstechnica.com/information-technology/2020/02/google-removes-reinstates-and-removes-totok-app-said-to-spy-for-uae-government/

Graff, Garrett M. 2020. "China's Hacking Spree Will Have a Decades-Long Fallout." *Wired*, February 11. www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/.

Hartzog, Woodrow. 2018. *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Cambridge, MA: Harvard University Press.

Herrman, John. 2019. "How TikTok Is Rewriting the World." *The New York Times*, March 10. www.nytimes.com/2019/03/10/style/what-is-tik-tok.html.

Hill, Kashmir. 2020. “The Secretive Company That Might End Privacy as We Know It.” *The New York Times*, January 18. www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

Hsu, Jeremy. 2018. “The Strava Heat Map and the End of Secrets.” *Wired*, January 29. www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.

Hu, Minghe. 2019. “China issues rules to stop apps from abusing user’s personal information in latest data privacy effort.” *South China Morning Post*, December 31. www.scmp.com/tech/apps-social/article/3044051/china-issues-rules-stop-apps-abusing-users-personal-infor

Jackson, James K. and Cathleen D. Cimino-Isaacs. 2020. “CFIUS Reform Under FIRRMA.” Congressional Research Service, February 21. https://fas.org/sgp/crs/natsec/IF10952.pdf.

Landau, Susan. 2018. “Understanding Data Breaches as National Security Threats.” *Lawfare* (blog), February 26. www.lawfareblog.com/understanding-data-breaches-national-security-threats.

Lewis, Jeffrey. 2018. “Fitness-Tracker App Exposes Security Flaw at Taiwan’s Missile Command Center.” The Daily Beast, January 29. www.thedailybeast.com/strava-fitness-tracker-app-exposes-taiwans-missile-command-center.

Lipman, Rebecca, Online Privacy and the Invisible Market for Our Data (January 18, 2016). 120 Penn State Law Review 777 (2016). Available at SSRN: https://ssrn.com/abstract=2717581

Liptak, Andrew. 2018. “Strava’s fitness tracker heat map reveals the location of military bases.” The Verge, January 28. www.theverge.com/2018/1/28/16942626/strava-fitness-tracker-heat-map-military-base-internet-of-things-geolocation.

McLaughlin, Jenna. 2017. “Deep Pockets, Deep Cover: The UAE is paying ex-CIA officers to build a spy empire in the Gulf.” *Foreign Policy*, December 21. https://foreignpolicy.com/2017/12/21/deep-pockets-deep-cover-the-uae-is-paying-ex-cia-officers-to-build-a-spy-empire-in-the-gulf/.

McLaughlin, Jenna and Zach Dorfman. 2019a. “Exclusive: Pentagon warns military members DNA kits pose ‘personal and operational risks.’” Yahoo News, December 23. https://news.yahoo.com/pentagon-warns-military-members-dna-kits-pose-personal-and-operational-risks-173304318.html?soc_src=hl-viewer&soc_trk=tw.

Murphy, Hannah, 2020. “TikTok accused of breaching US child privacy regulations,” Ars Technica, May 14, https://arstechnica.com/tech-policy/2020/05/tiktok-accused-of-breaching-us-child-privacy-regulations/?comments=1

National Academy of Sciences. 2015. *Privacy Research and Best Practices: Summary of a Workshop for the Intelligence Community*. Washington, DC: The National Academies Press. www.nap.edu/catalog/21879/privacy-research-and-best-practices-summary-of-a-workshop-for.

National Counterintelligence and Security Center. 2020. *National Counterintelligence Strategy of the United States of America 2020–2022*. February. www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf.

Neal, Meghan. 2013. “The Defense Department Thinks Troves of Personal Data Pose a National Security Threat.” Vice, August 13. www.vice.com/en_us/article/9aax5p/the-defense-department-thinks-troves-of-personal-data-pose-a-national-security-threat.

Newcomb, Alyssa. 2019. “Why Apple and Google Have ‘No Real Way’ to Stop Surveillance Apps Like ToTok.” *Fortune*, December 23. https://fortune.com/2019/12/23/apple-google-surveillance-apps-totok/.

Nicas, Jack, Mike Issacs and Anna Swanson. 2019. “TikTok Said to Be Under National Security Review.” *The New York Times*, November 1. www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html.

Ohm, Paul. 2010. “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization.” *UCLA Law Review* 57: 1701–78. https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1016&context=hightechevents.

On Point. 2019. “FaceApp: Age Your Photos — And Compromise Your Privacy?” July 22. www.wbur.org/onpoint/2019/07/22/faceapp-aging-photos-russia-privacy-security.

Office of the Privacy Commissioner of Canada (OPC). 2014a. *Metadata and Privacy: A Technical and Legal Overview*. October. www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md_201410/#fn10.

Overly, Steven. 2019. “TikTok emerges as Silicon Valley’s scapegoat in Washington.” Politico, November 5.

www.politico.com/news/2019/11/05/tiktok-silicon-valley-scapegoat-in-washington-066339.

Parsons, Christopher, Adam Molnar, Jakub Dalek, Jeffrey Knockel, Miles Kenyon, Bennett Haselton, Cynthia Khoo and Ron Deibert. 2019. *The Predator in Your Pocket, A Multidisciplinary Assessment of the Stalkerware Application Industry*. Citizen Lab, June 12. https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/.

Privacy Int'l, A Race to the Bottom: Privacy Ranking of Internet Service Companies (Sept. 9, 2007), available at http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-553961.

Robb, Drew. 2017. "Building the Global Heatmap." November 1. https://medium.com/strava-engineering/the-global-heatmap-now-6x-hotter-23fc01d301de.

Sacks, Samm. 2020. "Dangerous Partners: Big Tech and Beijing." Committee on the Judiciary, Subcommittee on Crime and Terrorism, March 4. www.judiciary.senate.gov/imo/media/doc/Sacks%20Testimony.pdf.

Scott-Railton, John and Andrew Hilts. 2018. "Fit Leaking: Citizen Lab Research on Fitness Tracker Privacy." Citizen Lab, January 29. https://citizenlab.ca/2018/01/fit-leaking-citizen-lab-research-fitness-tracker-privacy/.

Sly, Liz. 2018. "U.S. soldiers are revealing sensitive and dangerous information by jogging." *The Washington Post*, January 28. www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html.

Smith, Allan. 2019. "TikTok and China come under scrutiny in congressional hearing." NBC News, November 5. www.nbcnews.com/politics/congress/hawley-takes-aim-tiktok-china-congressional-hearing-n1076586.

Sonnad, Nikhil. 2015. "The Chinese military is afraid wearables will reveal its secrets." Quartz, May 11. https://qz.com/402353/the-chinese-military-is-afraid-wearables-will-reveal-its-secrets/.

Thompson, Stuart A. and Charlie Warzell. 2019. "How to Track President Trump." *The New York Times*, December 20. www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html.

UN Human Rights Council, 2019. Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, May 28, A/HRC/41/35.

Van Puyvelde,Damien, Shahriar Hossain and Stephen Coulthart, National security relies more and more on big data. Here's why. Washington Post, September 27, https://www.washingtonpost.com/news/monkey-cage/wp/2017/09/27/national-security-relies-more-and-more-on-big-data-heres-why/

Wall Street Journal. 2020. "TikTok to Stop Using China-Based Moderators to Monitor Overseas Content." March 15. www.wsj.com/articles/tiktok-to-stop-using-china-based-moderators-to-monitor-overseas-content-11584300597.

Warwick, Stephen. 2019. "ToTok co-founder pleads with Apple and Google to reinstate its app." iMore, December 31. www.imore.com/totok-co-founder-pleads-apple-and-google-reinstate-messaging-app.

Zuboff, Shoshana. 2019. The Age of Surveillance Capitalism, New York Hachette.