Institute for International Economic Policy Working Paper Series
Elliott School of International Affairs
The George Washington University

Data Is Dangerous: Comparing the Risks That the United States, Canada and Germany See in Data Troves

IIEP-WP-2020-5

Susan A. Aaronson
George Washington University

April 2020

Institute for International Economic Policy
1957 E St. NW, Suite 502
Voice: (202) 994-5320
Fax: (202) 994-5477
Email: **iiep@gwu.edu**
Web: **iiep.gwu.edu**

Centre for International
Governance Innovation

CIGI Papers No. 241 — April 2020

Data Is Dangerous

Comparing the Risks That the United States, Canada and Germany See in Data Troves

Susan Ariel Aaronson

Centre for International
Governance Innovation

CIGI Papers No. 241 — April 2020

Data Is Dangerous

Comparing the Risks That the United States, Canada and Germany See in Data Troves

Susan Ariel Aaronson

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches evaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Director, Global Economy Robert Fay
Program Manager Heather McNorgan
Publications Editor Susan Bubak
Senior Publications Editor Jennifer Goyder
Graphic Designer Brooklynn Schwartz

For publications enquiries, please contact publications@cigionline.org.

Printed in Canada on Forest Stewardship Council® certified paper containing 100% post-consumer fibre.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Author

Susan Ariel Aaronson is a CIGI senior fellow. She is an expert in international trade, digital trade, corruption and good governance, and human rights. She is currently writing papers on global digital trade rules, artificial intelligence as a global public good and the governance of data markets.

In addition to her work at CIGI, Susan is a research professor of international affairs and cross-disciplinary fellow at George Washington University's Elliott School of International Affairs, where she directs the Digital Trade and Data Governance Hub. The Hub educates policy makers and the public on domestic and international data governance.

Susan is the former Minerva Chair at the National War College. She is the author of six books and numerous articles. Her work has been funded by major international foundations including the MacArthur Foundation, the Ford Foundation and the Rockefeller Foundation; governments such as the Netherlands, the United States and Canada; the United Nations, International Labour Organization and the World Bank; and US corporations including Google, Ford Motor and Levi Strauss.

Susan is also a frequent speaker on public understanding of globalization issues and international economic developments. She regularly comments on international economics on *Marketplace* and was a monthly commentator on *All Things Considered* and *Morning Edition*. Susan has appeared on CNN, CBC, the BBC and NPR to discuss trade and globalization issues. From 1995 to 1999, she was a guest scholar in economics at the Brookings Institution, and from 2008 to 2012, she was a research fellow at the World Trade Institute. In her spare time, Susan enjoys triathlons and ballet.

Acronyms and Abbreviations

AAAS	American Association for the Advancement of Science
AI	artificial intelligence
CFIUS	Committee on Foreign Investment in the United States
FBI	Federal Bureau of Investigation
FIRRMA	Foreign Investment Risk Review Modernization Act
FTC	Federal Trade Commission
GAO	Government Accountability Office
GWU	George Washington University
IP	intellectual property
IS	Islamic State
OPC	Office of the Privacy Commissioner of Canada
OPM	Office of Personnel Management
UAE	United Arab Emirates
UNICRI	United Nations Interregional Crime and Justice Research Institute

Executive Summary

Citizens of the United States, Canada and Germany know that the online world is simultaneously a wondrous and dangerous place. They have seen details about their activities, education, financial status and beliefs stolen, misused and manipulated.

This paper attempts to examine why stores of personal data (data troves) 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 rely on many of the same data-driven services and give personal information to many of the same companies. German and Canadian policy makers and scholars have also warned of potential national security spillovers of large data troves.

However, the three nations have defined and addressed the problem differently. US policy makers see a problem in the ownership and use of personal data (*what and how*) instead of in America's own failure to adequately govern personal data. The United States has not adopted a strong national law for protecting personal data, although national security officials have repeatedly warned of the importance of doing so. Instead, the United States has banned certain apps and adopted investment reviews of foreign firms that want to acquire firms with large troves of personal data. Meanwhile, Canada and Germany see a different national security risk. They find the problem is *where and how* data is stored and processed. Canadian and German officials 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).

The case studies illuminate a governance gap: personal data troves held by governments and firms can present a multitude of security risks. However, policy makers have put forward nationalistic solutions that do not reflect the global nature of the risk.

Introduction

Americans, Canadians and Germans have seen first-hand that the online world is both a wondrous and dangerous place. For example, in July 2015, a hacking group calling itself "the Impact Team" stole the user data of Ashley Madison, a commercial website based in Canada. The website promised to facilitate "dates," in particular extramarital affairs.[1] The hackers threatened to release users' names and personally identifying information unless the site shut down.[2] Soon thereafter, the hackers leaked details of some of the company's 40 million global users, as well as maps of internal company servers, employee network account information, company bank account data and employee salary information.[3] Over the next few months, many of these users in Canada and globally were subjected not only to embarrassment but also extortion and phishing attempts.[4]

In 2016, the huge Chinese game developer Beijing Kunlun Tech Co. purchased Grindr LLC, a dating app based in the United States.[5] The firm was likely attracted to Grindr because, with more than 20 million users, it is the world's largest social networking app for LGBTQ people.[6] However, on April 2, 2018, Buzzfeed News reported that the new owner of Grindr was sharing information about its users with two analytics companies, which could then sell this information.[7] The next day, US Senators Edward Markey and Richard Blumenthal demanded the company explain how it protected the personal data of its users.[8]

1 See PR Newswire (2016). Avid Life Media Inc. is headquartered in Toronto, Ontario. The company owns and operates various dating advertising brands and websites.

2 See Krebs (2015a).

3 See Bushatz (2015); Reuters (2015).

4 See Krebs (2015b); Gregoire (2015).

5 Beijing Kunlun Tech Co., Ltd. is one of China's biggest companies engaged in the development and distribution of online games. In addition, the company is also involved in the agency distribution of online games developed by other companies, as well as the operation of software application stores. The company distributes its products in domestic and overseas markets (see www.reuters.com/companies/300418.SZ).

6 Grindr holds a lot of sensitive data about its users, including what they look like, relationship status, ethnicity, age, gender, pronoun preference, email address, height, weight, body type and HIV status (see www.grindr.com/about/; www.grindr.com/privacy-policy/#collect).

7 See Ghorayshi and Ray (2018).

8 See Markey and Blumenthal (2018).

Box 1: Terminology

Data brokers can be defined as a business or business unit "that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship" (Strawbridge 2018).

Data governance refers to the norms, principles and rules governing the treatment of data. The author defines personal data protection as steps taken through regulations, laws and policies to protect personally identifiable information that can be used to determine a person's identity.

Data troves are large stores of various types of data such as personal data.

National security refers to the requirement to maintain the legitimacy and survival of the state. In a viable and healthy nation, citizens trust their government, live in a stable and growing environment, and generally feel safe and secure. Security threats can include warfare, terrorism, economic conflict, digital attacks, malicious non-state actors such as drug cartels, natural disasters, environmental degradation and contagious diseases (Science Daily 2019; American Association for the Advancement of Science [AAAS], Federal Bureau of Investigation [FBI], and United Nations Interregional Crime and Justice Research Institute [UNICRI] 2014).

Privacy and personal data protection are related concepts, but they are not the same. Individuals have a basic human right to keep their information private, whereas data protection relates to the protection of data as it is processed often by governments or outside firms — so-called third parties (Abrams 2019). While there is an internationally accepted right to privacy, countries have different interpretations of the right to privacy online. These differences have coloured domestic regulation of data. For example, European privacy law is built on the belief that sensitive information about an individual must not be collected or used without their knowledge and permission. The default US position is that sensitive information about an individual *can* be collected or until a law or lawsuit says it *should not* be collected (Cobb 2018). There is no internationally accepted right to personal data protection per se, but some countries/common markets such as Brazil, Mexico and the European Union have given their citizens this new right under law.

Third parties can be firms or governments that want to use or sell personal data.

A slightly chastened management said it would stop sharing this sensitive information, but only after it released a new version of its app.[9] The company next announced it would consolidate operations in Asia and granted Asian engineers access to the Grindr database for several months (Ghorayshi and Ray 2018). The company also switched some of its communications over to the Chinese messaging app WeChat, which is not encrypted.[10] Chinese companies are often required to share personal data with the Chinese government (Sacks 2020). Hence, with these steps, Grindr's new owners showed their commitment to personal data protection was at best uneven.

Finally, in January 2019, the German government discovered that a hacker or hacking group had published sensitive personal data belonging to German politicians, celebrities and public figures online via a Twitter account. The hack also included the personal details of European parliamentarians. The huge cache of documents included phone numbers and addresses, internal party documents, credit card details and private chats.[11]

9 See Ghorayshi (2018).

10 See Rosenberg (2019).

11 See Le Blond (2019); Connolly (2019).

Although these three incidents are different, they provide examples of how the theft or misuse of large stores of personal data (data troves) held by private firms can create security risks at the individual, national and international level. These threats can be indirect or direct and presented by insiders (domestic citizens or firms) or outsiders (foreign firms or adversaries). Moreover, data troves can be hacked, stolen and manipulated. Data troves can also be crossed to identify individuals, putting their personal security at risk.

Meanwhile, individuals rely on computer and mobile phone applications that collect data about their activities and movements. When collected and anonymized, such aggregated data held in private firms' data troves can reveal information about a government's objectives and strategies. Thus, governments are also vulnerable when personal data held by governments or firms can be hacked or stolen and then compiled, analyzed and even monetized.

Hackers and adversaries are eager to get at these personal data troves.[12] The US Cyberspace Solarium Commission (2020, 93) noted, "The loss or exposure of sensitive information is becoming more common and more severe."

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 rely on many of the same data-driven services and give personal information to many of the same companies. German and Canadian policy makers and scholars, like those in the United States, have warned of potential national security spillovers of large data troves. However, Canadian and German officials are more focused on a different national security risk — the infrastructure where data is stored and processed. They want to ensure that Canadian and German laws apply to Canadian and German personal or government data when it is stored on the cloud.

Some analysts have begun to examine and report on the national security implications of these data troves (Cordero 2018; Biancotti 2019; Albrycht 2020; Thompson and Warzell 2019). However, this is the first study to examine this issue in depth. The author uses 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 paper examines five cases where a US government official or agency asserted that a trove of data presented a national security risk. The cases include social networks and applications available on smartphones. Each of these social networks or apps is available in Germany and Canada as well as the United States.

The cases provide examples of the complex interactions of the data-driven economy. 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; they create trust and value by facilitating dialogue between users and firms and hence play a leading role in moving personal data. Apps can make texting easier, direct individuals to voting sites or water supplies, help put users to sleep, or monitor their digital footprint. App creators often use the personal data provided to create new products and services built on data. But like social network firms, they can also sell the data they acquire.[13]

While netizens in the United States, Canada and Germany all use these social networks and apps, they do not have the same protections for their personal data. The United States lacks a national personal data protection law. As of this writing, although the United States does protect personal data through sectoral laws (such as laws regulating health data), state legislators are trying to fill in the gaps with state legislation. The United States does, however, have relatively strong tools of enforcement. Meanwhile, Canada has a strong personal data protection law, but has relatively weak tools of enforcement, according to the

12 An analysis of such hacks by the Center for Strategic and International Studies finds that there were some 104 major cyber events from March 2019 to March 2020, and some 15 involved the theft of personal data from government entities and private firms. In 2006–2008, the report details none – back then, hackers wanted to disrupt or steal intellectual property (IP) (see https://csis-prod.s3.amazonaws.com/s3fs-public/200306_Significant_Cyber_Events_List.pdf?qRZXF65CUUOKTOl9rLVBMJhXfXtmJZMj).

13 The US app economy in 2018 was estimated to be worth US$568.47 billion, including 317,673 companies and some 5,744,481 jobs, according to the accounting firm Deloitte (2018, 3–5, 17).

Table 1: Free App Popularity in Germany, Canada and the United States

	Germany, Dec. 31, 2019	Germany, April 8, 2020	Canada, Dec. 31, 2019	Canada, April 8, 2020	United States, Dec. 31, 2019	United States, April 8, 2020
Facebook	18	48	16	44	19	44
Strava	-	96	-	-	-	-
FaceApp	360	-	-	-	-	-
ToTok	-	-	-	-	-	-
TikTok	11	4	2	5	5	3

Source: Data from App Annie, a free (and paid) website that provides intelligence on the app sector and its customers (see www.appannie.com/en/). Table by Charlene Burns, research assistant at George Washington University.

Office of the Privacy Commissioner of Canada (OPC). Germany, as part of the European Union, has a very strong and comprehensive approach to personal data protection, but so far has not been effective at ensuring enforcement.[14]

Table 1 gives readers a sense of the popularity of these social networks and apps over time, based on downloads from Apple's App Store. The table lists their position among the top 500 free apps in each country on December 31, 2019, and then on April 8, 2020. App popularity varies over time in response to social, economic and technological developments, and store conditions/rules.

The author does not contend that these five cases present a representative sample, which would be hard to discern. 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 broker firms, such as Experian, which buy and sell personal data. Nonetheless, these cases provide a "most different" design, whereby there is considerable variation across internet application, country (countries), personal data protection laws and alleged effects on national security (direct or indirect, insider or outsider).[15]

This paper is organized as follows. The author begins by showing that although adversaries have long used personal data to gain an advantage, policy makers first began to identify the risks in the last eight to 10 years (2012–2020). The author next briefly discusses the relationship between personal data governance and security in the United States and what factors colour that relationship. The author then discusses specific cases (Table 2 provides an overview of each case). Next, the author examines the American policy response in 2018–2020. The author then describes the national security threat envisioned by German and Canadian policy makers and presents some conclusions.

What Kinds of Threats Are Posed by Inadequate Governance of Personal Data?

Throughout history, some individuals have threatened to reveal private information to prod another person to change their behaviour. Moreover, adversaries have historically used disinformation to undermine trust and societal cohesiveness (Hu 2012; Lucas 2019). With global adoption of the internet, the world is flooded with data, including personal data, making the potential to misuse data infinitely more complex. In addition, the world is seeing the following developments:

14 See Fennessy (2019); see also 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, comparing Canada and the United States. On Office of the Privacy Commissioner of Canada (OPC), see OPC (2019a).

15 Yet other data-driven threats are emerging, such as biometric passports (Longo 2020).

Table 2: Overview of Cases Discussed

Case	Country/Countries Affected	Type of Data Service/Platform	Data Governance Problem(s)	Threat to US National Security
Facebook	Global/ United States	Social network	Inadequate protection of personal data and the sale of personal data	Insider threat: violation of privacy, distrust
Strava	Global/ United States	Social network for athletes	Inadequate understanding of spillover effects of exposure of collective anonymized personal data	Insider threat: exposure of anonymized personal information of military, exposed national security information
FaceApp	Global/ United States	Photo app created in Russia that ages users' photos	Inadequate governance of personal data	Outsider threat: could share data with Russia and/or other adversaries
ToTok	Global/ United States	Messaging app created in the United Arab Emirates (UAE)	App designed to surveil and provide personal data	Outsider threat: government-appropriated app to surveil
TikTok	Global/ United States	Video-making and viewing app created in China	Acquisition of personal data	Outsider threat: data sets could be crossed, used for blackmail, intimidation

Source: Author.

- **Transition to a data-driven economy:** Many middle-income and wealthy countries are transitioning toward economies built around the collection, preservation, protection, implementation and understanding of many different types of data, including personal, public, machine, satellite and proprietary data (World Economic Forum 2011).
- **Rising demand for data sets:** Researchers, officials and firms using new technologies such as artificial intelligence (AI) or data analytics need large and often multiple troves of data to solve complex problems. When they use these technologies, they vacuum and cross large data sets. As the demand for data rises and the supply of data and data sets grows, 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,[16] collect and store extensive data about their users (Amnesty International 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 and many data processes will shift from centralized computing facilities to smart connected devices. The European Commission estimates that the volume of global data is expected to grow from 33 zettabytes in 2018 to 175 zettabytes in 2025 (European Commission 2020). A zettabyte is 1,000,000,000,000,000,000,000 bytes.

16 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.

- **Rise of tracking:** 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 Team 2018). In 2018, *The New York Times* reported that at least 75 companies receive anonymous, precise location data from mobile apps.[17]

- **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). Some argue that this opacity leads to "too much data collection and too little privacy" (Carrière-Swallow and Haksar 2019). In the United States, without strong privacy laws and enforcement, consumers are often unable to protect, correct or prevent the sale of their personal data (Federal Trade Commission [FTC] 2014, 13-14, 17). Despite having strong data protection laws, the European Union also does not directly regulate data markets and the work of data brokers.[18] Canada also does not directly regulate data brokers or data markets. In 2014, the OPC warned "the use of cloud computing raises concerns about data brokers' ability to demonstrate accountability, safeguard information, and manage risks associated with transborder dataflows and foreign jurisdiction" (OPC 2014b).

- **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.[19] Dell also found that in 2018 and 2019, the total cost of data loss through theft, manipulation and other causes averaged almost US$1 million per organization.[20]

- **Inadequate governance and control over public data sets:** In recent years, many states have come to rely on data-driven services such as apps and AI to understand and shape the international environment (Carter 2019). In so doing, these nations have created and/or tapped personal data provided by and about their citizens. However, information about their citizens' activities and movements can reveal information about a governments' objectives and strategies. Thus, governments are also vulnerable when personal data held by governments or firms can be hacked or stolen and then compiled, analyzed and even monetized.

- **Inadequate self-regulation:** Companies have many incentives to utilize and monetize data and fewer incentives to protect data, despite its effects on trust. Facebook provides a good example: despite its consistent failure to protect its users, its user base kept growing.[21]

- **A plethora of bad actors in cyberspace:** These actors, including authoritarian governments, hackers and criminals, can easily hide from the reach of international law.[22]

- **Data is easy to exploit:** For example, during the 2016 US presidential election, Russian operatives purchased stolen US identities, which they used to open US bank and PayPal accounts and to buy access on US-based servers; they then 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, including the United States, Canada and Germany, are relatively open to foreign investment.[23] Adversaries can take advantage of this openness and use front companies, joint ventures, mergers and acquisitions, and direct investment to gain access to data troves (Office of the Director of National Intelligence 2020).

17 See Valentino-DeVries et al. (2018).

18 See Ram and Murgia (2019).

19 Dell surveyed 2,200 information technology decision makers from public and private organizations located in Europe, Asia and the Americas in 2018 (see Dell Technologies 2018, slides 1–3, 10, 21, 34, 35). Dell updated the study in 2020 and found firms were especially struggling to protect new technologies such as AI (see www.delltechnologies.com/en-us/data-protection/gdpi/index.htm#gdpi_2020).

20 Ibid.

21 See Hutchinson (2019).

22 See National Security Agency Central Security Service, n.d.

23 See Law360 (2019).

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

In October 2013, Vietnamese national Hieu Minh Ngo was indicted in the United States on charges that he managed an international identity theft scheme. Ngo created a website called superget.info, which let users search the Social Security numbers, birthdates and other identity assets of millions of Americans. In so doing, he helped make cybercrime a fee-based service, where users could purchase this data, resell it, or use it to file fraudulent tax returns, apply for benefits or drain bank accounts (Bailey, n.d.).

That same year, 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.[24] 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 hacked or legally purchased from US and foreign firms.[25]

Meanwhile, scientific groups such as the AAAS and the National Academy of Sciences, as well as the Office of the Director of National Intelligence began warning that big data posed potential national security risks. The AAAS recommended that the government "develop scenarios to identify existing legal, technological, institutional, and individual solutions and gaps in governance that need addressing. This should include support for the development of 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; National Academy of Sciences 2015).

US policy makers also discovered that adversaries could monitor individual members of the military online and use their personal information to target them. In 2014, *The New York Times* reported that a group linked to the Islamic State (IS), calling itself the Islamic State Hacking Division, released a "hit list" containing the personal information of 100 current and former American military service members. The personal information included the names and addresses, along with photos, of military personnel who had fought against the IS. In 2014, in response, officials from the FBI and the Department of Homeland Security urged members of the military to scrub their social media accounts of anything that might bring unwanted attention from "violent extremists" or would help extremists learn individual service members' identities.[26] Members of the US military in Kuwait were targeted again in 2020.[27]

Finally, during the administration of Barack Obama (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 2018). Moreover, China seemed to excel at stealing IP. Finally, China had also begun to steal personal data from both government and private sector firms. According to Aspen Institute Scholar Garrett Graff (2020), "Chinese intelligence has amassed in just five years a database more detailed than any nation has ever possessed about one of its adversaries. The data and its layers 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." Arguing that 80 percent of US cyber thefts were attributable to China, the US Department of Justice launched the "China Initiative" in

24 See Sternstein and Moore (2015).

25 See Fruhlinger (2020). While no "smoking gun" was found linking the attack to a specific perpetrator, the overwhelming consensus is that the OPM was hacked by state-sponsored attackers working for the Chinese government. Among the evidence is the fact that PlugX, the backdoor tool installed on OPM's network, is associated with Chinese-language hacking groups that have attacked political activists in Hong Kong and Tibet; the use of superhero names is also associated with groups tied to China. See also Stone Fish (2019).

26 See https://identity.utexas.edu/id-perspectives/isis-targeting-military-members-via-social-media.

27 See Rempfer, Snow and Altman (2020).

November 2018, with the aim of countering Chinese national security threats, including trade secret and IP theft, hacking and economic espionage.[28]

The United States was particularly attuned to the issue of data troves as a national security problem for several reasons: it has a large overstretched military, as well as many of the world's largest data-driven firms with global reach. But it also had a substantial gap in good data governance. Most countries have adopted personal data protection rules that provide their citizens with some rights to control the use of their data (UNCTAD 2019). The United States has strong rules governing *governmental* use and storage of data, as well as rules governing sectoral use of personal data. But the United States has no national personal data protection law (O'Connor 2018; Department of Homeland Security 2017). Moreover, according to the US Government Accountability Office (GAO), 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 and travel routes, might affect national security (GAO 2019). 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 — A Direct Insider Threat: Facebook and Its Users' Data

The director of platform partnerships at Facebook was blunt. In his November 2019 blog post,[29] Konstantinos Papamiltiadis admitted that yet again, the company had been sloppy in allowing other firms and researchers to reuse and misuse personal data.[30] Because Facebook has so many users around the world, its practices affect many firms and netizens and influence the behaviour of its many advertisers.

Facebook is an internet behemoth. Some 2.2 *billion* people use Facebook and/or its messaging apps WhatsApp, Instagram, or Messenger each day on average (Amnesty International 2019; Noyes 2019). Many rely on Facebook not only to send messages or to catch up with their friends and family but also for hard news. However, because many believe the site does not adequately police its users and advertisers, the satirist Sacha Baron Cohen recently described the company as "the greatest propaganda machine in history" (Baron Cohen 2019).

With influence comes responsibility, but Facebook has a long history of inadequately protecting personal data. Although Facebook claims its users are its top priority, its clients are not its users. Facebook's clients are instead the many advertisers and other companies that want access to its users' data (Gilbert 2018; Frenkel et al. 2018). For example, when Facebook opened up its social network to third-party developers, enabling them to build apps that users could share with their friends, it allowed them to plug into user accounts and download a wealth of personal data. Cambridge Analytica used this information to advise its clients and influence elections around the world in ways that threatened democracies and economic stability (Kulwin 2018; Amnesty International 2019).

Facebook did not embed personal data protection in its initial design because it takes its users' personal data, anonymizes and aggregates it, and then sells this anonymized, aggregated data to its global customers (other firms, advertisers, data brokers and so forth) (Hartzog 2018). As evidence that Facebook depends on inadequate governance of this personal data, the company did not put forward a set of privacy principles to guide its practices until 2019. Yet despite the establishment of these principles, the company continues to misuse personal data.[31]

28 See Hungerford (2019).

29 Papamiltiadis (2019) stated, "Some apps retained access to group member information, like names and profile pictures…from the Groups API, for longer than we intended."

30 Facebook claims it has a social purpose — the company and its products are designed to bring the world closer together. In a 2012 letter to investors, the company stated, "We hope to change how people relate to their governments and social institutions. We believe building tools to help people share can bring a more honest and transparent dialogue around government that could lead to more direct empowerment of people, more accountability for officials and better solutions to some of the biggest problems of our time" (Reuters 2012).

31 See www.facebook.com/about/basics/privacy-principles.

Facebook's failure to protect personal data not only affects the human rights and autonomy of its users but it directly affected national security in the United States and other nations. In 2016, the company knew, but did not inform US government officials, that Russian hackers routinely penetrated the site and attempted to find data on staffers affiliated with presidential campaigns (Frenkel et al. 2018).[32] On April 4, 2018, *The Washington Post* reported that Facebook announced "malicious actors" abused its search function to gather public profile information of "most of its 2 billion users worldwide" (Sanders and Patterson 2019). On June 5, 2018, *The Washington Post*[33] and *The New York Times* reported that the Chinese device manufacturers Huawei, Lenovo, Oppo and TCL were granted access to user data under this program. Huawei, along with ZTE, is considered a national security risk.[34] Moreover, on January 17, 2019, Facebook disclosed that it removed hundreds of pages and accounts controlled by Russian propaganda organization Sputnik, including accounts posing as those belonging to politicians from primarily Eastern European countries.[35]

The US military considers social media networks such as Facebook both a threat and a useful source of information. In 2015, the US Special Operations Command announced that it would build a new data-mining tool capable of crawling data from "pre-determined web sites" to "support geospatial, temporal, relationship, textual, and multi-media visualization and visual analytics." The strategy would enable greater situational awareness in combat zones (Tucker 2015).

Government officials in Canada and the European Union are well aware of the threat posed by Facebook's inability and unwillingness to protect personal data or prevent disinformation. In March 2018, in response to a complaint, the OPC investigated Facebook and found that the company failed to get meaningful consent from users or friends of users, it inadequately protected user privacy and it was not effectively held to account for these failures. The OPC learned from this process. Because the OPC could not levy a significant fine, it called for stronger privacy laws in Canada and more authority for regulators to inspect and penalize companies (OPC 2019). In May 2019, Canada hosted an International Grand Committee of parliamentarians seeking solutions to these challenges in the aftermath of investigations into Facebook and Cambridge Analytica. The committee, made up of representatives from 11 countries, declared that social media platforms should strengthen privacy rights and data protections and that regulation may be necessary to achieve this.[36]

Facebook is under investigation by the European Union for violating EU data protection laws. In February 2019, a German state court in Berlin ruled that some user terms set by Facebook violated these laws.[37]

In sum, the social networking site Facebook threatens national security because it is unwilling to effectively protect the many types of data it obtains from users. Facebook has not yet been incentivized to effectively protect personal data. However, interestingly, in the face of Chinese competition, it is supposedly transitioning to a new business model built on encryption.[38]

Case 2 — An Indirect Insider Threat: Strava's Use of Geolocation and Personal Fitness Devices and Its Impact on National Security

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). Strava is one of the most prominent social networking sites for athletes (it is also an app).[39] Individuals use Strava to record their activities and can compete against others for time or distance. 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).

32 See Select Committee on Intelligence, n.d.

33 See Romm (2018).

34 See LaForgia and Dance (2018); Sanders (2018).

35 See Cimpanu (2019).

36 See OPC (2019b).

37 See Germano (2020); Perper (2018).

38 See Dwoskin (2019).

39 Strava (Swedish for strive) claims 46 million athletes from 195 countries upload training data to its site every week (see www.strava.com/).

The heat map did not get much attention beyond the fitness community until January 2018, when Nathan Ruser, then a grad student in Australia, reviewed the map and took to Twitter to publicize his concerns. He noted the operational security threat: "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.)[40] Some tweets described potential drone locations and alleged CIA black sites.[41]

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. As a result, the Strava heat map seemed to reveal 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 sources. One researcher claimed to use the heat map and other data sets to monitor the travels of a French solider from overseas deployment to the soldier's home (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. Moreover, as that soldier moves from base to base, the heat map reveals even more locations, which can be combined with other data sets to obtain additional national security data (Lewis 2018).

The publication of the heat map put the United States (and its allies) in a bind. On one hand, soldiers are encouraged to be physically fit, and athletic social networks can help them achieve fitness goals. In fact, the Pentagon distributed Fitbits as part of a pilot program to battle obesity in 2013 and 2015 (Sly 2018; Lilley 2015). Moreover, the US government has encouraged the military to use social media, including athletic networks, albeit cautiously. In 2015, it warned, "It's important to know what adversaries are looking for. Don't share your usernames, passwords, or network details. Don't share your job title, location, salary, or clearance level. Also avoid listing information about your home or work security and logistical details, like how you get to work and travel itineraries. Don't post information about your mission or your unit's capabilities and limitations....Listing your hobbies, likes, dislikes, etc., could be useful information to an enemy, especially for gaining trust and rapport before seeking other information."[42]

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 IS said it would revise its guidelines on the use of all wireless and technological devices: "The Coalition is in the process of implementing refined guidance on privacy settings for wireless technologies and applications, and such technologies are forbidden at certain Coalition sites and during certain activities" (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.[43]

Meanwhile, Strava rethought some of its applications (Goode 2018). The company wrote that it is "committed to working with the military and government officials to address potentially sensitive data."[44] Strava does have an option that allows users to hide the beginning and end of a workout. The company stresses it does not and has never tracked activity in the background, nor does it include private activities in the heat map (Meschke 2018).

The Strava case illustrates that aggregated, anonymized personal data can, at times, pose a national security threat. Governments are peering through such data to monitor and predict trends (for example, in the spread of ideas or disease).[45] The US government is also using anonymized data to predict behaviour and even monitor targets (Intelligence Advanced Research Projects Activity 2011; Tucker 2015). Interestingly, the Chinese government banned its military personnel from

40 Ruser's tweet and the responses can be found at https://twitter.com/Nrg8000/status/957318498102865920.

41 See https://twitter.com/AlecMuffett/status/957615895899238401.

42 See www.centcom.mil/VISITORS-AND-PERSONNEL/SOCIAL-MEDIA-SECURITY/; www.oge.gov/web/oge.nsf/0/16D5B5EB7E5DE11A85257E96005FBF13/$FILE/LA-15-03-2.pdf.

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

44 See Quarles (2018).

45 Interestingly, so far AI experts assert that AI is not very good at detecting social phenomena (Narayanan 2019).

using wearables on duty in 2015, in recognition that these devices might inadvertently reveal information on its activities (Sonnad 2015).

In 2018, researchers at Citizen Lab, a prominent Canadian research institution at the University of Toronto, analyzed Strava's heat map and data leakage from other fitness devices. They found:

- Users are often unaware that the privacy settings enabling them to hide things from strangers do not extend to their privacy from the platform they are using.
- Location privacy can be difficult for users to fully understand, and many devices and apps are more convenient to leave running than to disable.
- Companies that collect vast amounts of user data, such as fitness trackers, will invariably become attractive targets for government agencies and criminal organizations. Some governments may compel or coerce companies to turn over user data they collect, making these companies effectively "proxies" for state surveillance and espionage. If user data is improperly secured, criminals who are able to acquire the data can employ it for all ranges of fraud and abuse (Scott-Railton and Hilts 2018).

In addition, several studies have shown that anonymized data can be de-anonymized when researchers cross 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 the most senior government officials (such as US President Donald Trump) could be tracked using cellphone data from his Secret Service agents or those individuals who meet with him. "Like all data, the vast location files are vulnerable to hacks, leaks or sale at any point along that process. Multiple experts with ties to the United States' national security agencies warned in interviews that 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).

The US government has long been aware that location data can undermine personal security and national security. In 2012, the US GAO found that when firms collect and share location data, consumers are unaware they could be subject to increased surveillance when location data is shared with law enforcement, and they could be at higher risk of identity theft or threats to personal safety when companies retain location data for long periods or share data with third parties that do not adequately protect them (GAO 2012).

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.

Case 3 — An Outsider Threat: FaceApp

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, allegedly affiliated with the Russian government, claimed that users can "get magazine cover quality for any selfie with just a few taps! Improve your selfie or just have fun with gender swap, hair styling and other free amazing transformations."[46] FaceApp uses AI algorithms 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."[47]

Some 80 million users have downloaded the app since it first became available (Denham and Harwell 2019). In June, *The Washington Post* noted that because the app became popular so quickly, some observers feared that it might be a disinformation campaign (Fowler 2019). The Democratic National Committee warned individuals to delete the app (Denham and Harwell 2019).

In many ways, FaceApp is a typical app — it provides users with functions that go beyond the operating system of their smartphone or computer. And like many other apps, FaceApp was not designed to respect the privacy of users. A 2019 study of apps in India found that more than 95 percent of available mobile apps and websites in India share data with third parties without the user's permission. Many apps allow the firm

46 See https://apps.apple.com/us/app/faceapp-ai-face-editor/id1180884341.

47 See www.faceapp.com/terms-20170803.html.

providing the app to access the user's data and even access other phone utilities. For example, the permission for using certain apps allows them to read and access the user's contact list, use their microphone, access their location or mobile wallet, and see other personal details that could undermine personal safety or autonomy (Arkka 2019, 8, 10).

FaceApp was 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."[48] The company can then use the data it collects for its own purposes.

Not surprisingly, the CEO of FaceApp, Yaroslav Goncharov, sought to defend the company and its practices. He 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). In response to public concerns about FaceApp's approach to data, the company tightened its terms of service, but some analysts still viewed the app as a privacy risk. They note that the company retains control over the images that it processes. 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."[49]

As of this writing (March 2020), it is unclear if FaceApp is an arm of the Russian government, but the company's terms of use give it great power to control the information it collects. Moreover, the company plans to continue selling some of the data it has obtained. But it is not alone; US companies such as Clearview AI are also scraping the web and selling personal profiles to police authorities in both democratic and repressive states.

America's failure to enact clear personal data protection rules has enabled firms to obtain and monetize personal data for a wide range of current and future purposes. 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 do not regulate such permissions; they also rely on platforms to set and enforce the rules for app behaviour and use of personal data. However, as of this writing, neither Canada nor Germany identified FaceApp or similar applications as a national security threat.

Case 4 — An Outsider Threat: ToTok

ToTok (not to be confused with TikTok, discussed later) is a free messaging and calling app used by the UAE to spy on its citizens. 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 is also deliberately designed to spy on its users.

This app is available at a wide range of app stores. Apple, Google, Microsoft, Garmin and other companies first established app stores to provide users with apps, which can provide services and applications from text messaging, news and social networks. Many of these applications are free, where users agree to provide data in return for free services.

48 Ibid.

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

Apple, Google, Microsoft, Garmin and other companies with such stores derive many benefits from them. They can build trust and broader relationships with users, and get more data about the applications that users want and use. 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.[50] Nonetheless, developers can code malicious intent into their applications and evade the companies' rules (Newcomb 2019).

However, ToTok created a new and difficult challenge to app stores — policing alleged governmental use of personal data. 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, Perlroth and Bergman 2019).

The app is 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 individuals that use spyware can control and repress another individual, undermining their rights and autonomy (Parsons et al. 2019).

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 another Abu Dhabi-based cyber intelligence and hacking firm called Dark Matter.[51] 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 UAE has long relied on private firms to build its intelligence capacity (McLaughlin 2017).

Reuters and *Haaretz*, among others, have done in-depth studies of Dark Matter's operations. The firm has a sordid history of unethical behaviour.[52] In January 2019, Reuters found that Dark Matter had long used state-of-the-art cyber espionage tools to spy on human rights activists, journalists and political rivals. The company employed former US and Israeli intelligence and cyber security experts who shared spy-craft practices (McLaughlin 2017; Bing and Schectman 2019).[53]

The bulk of the company's operations is conducted out of a secretive compound known as "the Villa" in Abu Dhabi. Dark Matter claimed to take on only clients requesting defensive cyber security protection, but instead seems to target and surveil journalists, activists and others (Silverstein 2019). Some of those targeted by the firm are supposedly Americans (Ziv 2019; Silverstein 2019; Bing and Schectman 2019; Chesney 2019).

In 2017, Microsoft and Google, among others, granted Dark Matter provisional status to certify the safety of websites in 2017. But soon thereafter, Google and Mozilla blocked websites certified by Dark Matter from their browsers (Ziv 2019).

After two years of negative reportage about Dark Matter's operations, in 2019, the company's founders defended the app. They took no responsibility for the company's misuse of personal data and argued that their detractors were spreading misinformation: "Here is the fact — since day one, we have built ToTok with user security and privacy as our priority."[54] The company also claimed that the reason ToTok was allowed to operate in the UAE (apps such as FaceTime, WhatsApp and Skype are not available in the country) was that it was a pilot project that had met all the UAE's regulatory requirements. The company added, "We firmly deny this baseless accusation, and we are profoundly saddened by this complete fabrication that was thrown at us" (Warwick 2019). In early January 2020, the app was back on the Google Play site, but not on Apple's App Store.[55]

50 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/.

51 See Smith (2019).

52 Dark Matter is being investigated by the FBI (Bing and Schectman 2019).

53 Americans are banned from exporting intelligence training under the US International Traffic in Arms Regulations.

54 See https://totok.ai/news-dec24.

55 For Google, see https://play.google.com/store/apps/details?id=ai.totok.chat&hl=en_US. For Apple, see Hardwick (2019).

As of January 2020, the US government has not publicly warned users about ToTok or stated publicly that a foreign government created it or utilizes it. It is unknown whether the UAE created the app as alleged for surveillance purposes. But if these allegations are true, they show "proof of concept," and reveal how difficult it is to protect users from enticing apps designed to undermine and obtain a large pool of personal data. The author could find no information that other nations had banned ToTok, although the app seemed to violate app store guidelines.

Moreover, another government has utilized the app format to surveil its people. Vice News reported that Iran's Ministry of Health had created an app supposedly to inform Iranians about the coronavirus, but instead the app vacuumed up personal information. The app, called AC19, claimed to detect whether people are infected. Users are supposed to verify their phone number and then give the app permission to send precise location data to the government's servers (Gilbert 2020). It is ironic that AC19 and ToTok's misuse of personal data bolsters the national security arguments of the US government around apps, and yet, the US government has not banned either app.

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. The app has been downloaded more than 1.5 billion times. As users watch videos on the platform, the app uses AI to learn what users look for and then makes suggestions.

TikTok's parent company, ByteDance, describes its business as producing AI. But to some observers, the app looks like an enticing strategy to build a pool of personal data from users. In fact, ByteDance was fined by the US FTC in February 2019 because it found the company did not obtain parental consent before collecting children's personal data (Herrman 2019). The company agreed to pay US$5.7 million to settle the complaint. TikTok is still being investigated by the British Information Commissioner's Office to determine if it violated European privacy laws that offer special protections to minors and their data (Bergman, Frenkel and Zhong 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: Tiananmen Square, Tibetan independence and the religious group Falun Gong, for instance. *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 ongoing and widely publicized pro-democracy protests, which were a major topic on other social media sites at the time (Bergman, Frenkel and Zhong 2020). But it also came at a time when US companies were increasingly concerned about foreign (read Chinese) competition in data-driven services. Senator Josh Hawley described the company as "a Chinese-owned social media platform so popular among teens that Mark Zuckerberg is reportedly spooked" (Smith 2019). In congressional testimony, Matt Perault, then Facebook's head of global public policy,[56] testified that the company felt challenged by TikTok (Overly 2019).

Meanwhile, the US Army Recruiting Command began using the app to connect with new potential recruits. The command made social media part of its new recruiting strategy in 2019 when it missed its annual recruiting goal by 6,500 soldiers. The service announced in September that the app helped it surpass its recruiting goal for fiscal year 2019. Other branches of the US military allowed personnel to continue using the app (Cox 2019a).

In early October 2019, Senator Marco Rubio called for a formal investigation into whether TikTok poses a national security risk. Later that month, Senators Tom Cotton and Chuck Schumer 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).

But the executive branch was already concerned about the company. An arm of the US Treasury Department, the Committee on Foreign Investment in the United States (CFIUS), began to examine

56 See Lindsley (2019).

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 employees to "be wary of applications you download, monitor your phones for unusual and unsolicited texts, etc., and delete them immediately and 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 or using TikTok on government devices.[57]

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. Check Point concluded in its analysis that it is up to everyone to make data "safe from compromise." Meanwhile, TikTok addressed the vulnerability (Boxiner et al. 2020). TikTok offered Check Point a reward for finding the hole, but the company turned down the compensation.

While TikTok clearly has a problem protecting personal data, its rapid growth and new model certainly posed a threat to the market share of US competitors that provide 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 they indicated that user data could be shared "with any member or affiliate of [its] group" in China. TikTok later confirmed to him that "data from TikTok users who joined the service before February 2019 may have been processed in China," and hence such data may have been 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 (*The Wall Street Journal* 2020).

The United States stands alone in its concerns about the app. While other countries, such as the United Kingdom, have investigated the company, they have not implemented bans. TikTok remains popular in Germany and Canada, but these nations (and other governments) have not banned its use.

Recent US Policy Responses Appear Protectionist

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 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.[58] The law reflected congressional concern that the Treasury Department should carefully review any transaction that "is likely

57 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). Senator Josh Hawley has introduced legislation that would prohibit any federal employee from using or downloading TikTok on devices issued by the US government.

58 See www.treasury.gov/resource-center/international/Documents/Summary-of-FIRRMA.pdf.

to 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 in information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States." The president then banned "any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service (transaction) by any person…subject to the jurisdiction of the United States, where the transaction involves any property in which any foreign country or a national thereof has any interest (including through an interest in a contract for the provision of the technology or service), where the transaction was initiated, is pending, or will be completed after the date of this order."[59] 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 involving the sensitive personal data of US citizens if a firm could exploit such data in a manner that threatens US national security.[60] Such a review would depend on the sensitivity of the data, the sensitivity of the population about whom the data is maintained or collected, and whether the data can be used to distinguish or trace a person's identity. The Treasury developed 10 categories of review that might hold such data.[61]

The law made exemptions for investors from the United Kingdom, Canada and Australia because of the intelligence-sharing relationships among these countries. Policy makers also noted that other nations may be exempted following a review that will examine if such states have sufficient national security-based investment review processes and bilateral cooperation with the United States to merit such an exception.[62]

The Trump administration's approach to this issue was consistent with its approach to regulating AI under the Export Control Reform Act, also passed in 2018.[63] As with other US regulations, public comments were sought on how to limit the export of various types of AI. Many of the 268 comments warned against such controls.[64] At year end 2019, the Trump administration decided to limit only the export of certain AI-mapping applications.[65]

Meanwhile, 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).[66] Moreover, the United States rethought its counterintelligence strategy, recognizing that it must work with the private sector and research organizations to protect sensitive data. In 2020, the Office of the Director of National Intelligence announced it would engage and mobilize the private sector in protecting sensitive data, information and assets (Office of

59 See White House (2019).

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

61 They include a US business that:
- targets or tailors products or services to any US executive branch agency or military department with intelligence, national security or homeland security responsibilities;
- maintains or collects sensitive personal data for more than one million individuals at any point in a given 12-month period; or
- has a demonstrated business objective to maintain or collect sensitive personal data of more than one million individuals, and such data is an integrated part of the US business's products or services.

The 10 categories of sensitive personal data include genetic, biometric and medical data, and data pertaining to personal finances, personal communications and security clearances (see https://s3.amazonaws.com/public-inspection.federalregister.gov/2020-00188.pdf).

62 See Morrison & Foerster LLP (2020).

63 Both FIRRMA and the Export Control Review Act were part of the 2018 Defense Reauthorization Act (see www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf).

64 See Industry and Security Bureau (2018).

65 See Industry and Security Bureau (2020).

66 Interestingly, US intelligence agencies are trying to use such data (Fischer and Rosenberg 2019).

the Director of National Intelligence 2020, iii). But Congress continued to debate a national personal data protection law without arriving at a consensus. Despite increased attention to the risks of data troves, the United States has achieved no comprehensive solution.

A Brief Comparison with Canada and Germany

Like their American counterparts, Canadian and German officials are well aware that private troves of personal data could pose a national security threat if stolen or misused. These nations have strong personal data protection laws, but worry that Canadian and German firms do not own the cloud infrastructure where their data is stored and processed. Hence, these nations see a different threat to their national security.

Both countries are extremely open to foreign investment and competition in data-driven services. Neither nation has banned a particular app because it is foreign-owned or too loose with permissions.

In addition, neither Canada nor Germany has enacted foreign investment restrictions or reviews of firms that seek to merge with or acquire other firms with large troves of data.[67] Instead, the two countries have focused on clarifying their control over certain types of data stored in the cloud — what Canada calls data or Germany calls digital sovereignty.

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, 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 various types of data and where and how such data should be stored.[68] Non-Canadian cloud service providers can comply with these rules by ensuring that such data is stored in Canada. But such requirements might be considered a barrier to trade. In 2018, the Treasury Board (which advises the government) noted, "Canada cannot ensure full sovereignty over its data when it stores data in the cloud. Lack of full data sovereignty has the potential to damage the GC [Government of Canada] and third parties. Sensitive GC 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.[69]

Canada continues to debate the concept of data sovereignty. In 2019, Andrew Clement, professor emeritus at the University of Toronto, defined data sovereignty as an infrastructure problem. He claimed that Canada had little control over its data flows, noting that at least 25 percent of all internet communications in Canada was routed through the United States. He recommended that "all sensitive and critical Canadian domestic data be stored, routed and processed within Canada."[70] Influenced by his testimony, Parliament's Standing Committee on Public Safety recommended that "efforts to build out Canada's digital infrastructure can serve economic and national security interests concurrently. One important objective would be for Canada to enhance its connectivity with Europe and Asia, while reducing its reliance on the United States."[71]

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

67 The author researched this by examining the Canadian Centre for Cyber Security alerts and advisories and by doing a search of banned apps (see https://cyber.gc.ca/en/alerts-advisories).

68 See Treasury Board of Canada Secretariat (2018a).

69 See Treasury Board of Canada Secretariat (2018b).

70 Standing Committee on Public Safety and National Security (2019a).

71 Standing Committee on Public Safety and National Security (2019b), 42–46.

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 whether Canada will proceed along the lines of the United States in reviewing foreign investment in data-rich firms or banning certain practices.[72]

While Canada is still evolving its approach to protecting data through assertion of data sovereignty, Germany has a plan. Although the United Kingdom, Germany, France and other EU members have many competitive data-driven firms providing AI or cloud services, these firms are generally smaller than their US or Chinese counterparts (Aaronson and Leblond 2018; Aaronson 2019). Some in Europe see Europe's failure to establish a large, globally competitive cloud services sector as a security risk. 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. She argued that Europe would have to find its own path between the US approach, where giant companies dominate storing and processing data, and the Chinese approach, where the state controls and uses the data of its citizens (Chazen 2019). The German government explained that digital sovereignty is "the possibility of independent self-determination by the state and by organisations 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."[73]

That month, Germany announced that it would establish its own digital cloud through the "Gaia-X" project, which "aims at setting up a secure and trustworthy data infrastructure for Europe."[74] A spokesperson for Germany's economy ministry said that, in principle, the Gaia-X initiative will not exclude any company because it is not based in Europe; participating companies must, however, abide by European rules around data protection and "sovereignty." However, the spokesperson also noted that data governance rules are still to be defined.[75] Meanwhile, the director of EuroCloud Deutschland gave a different explanation: "Industry players in Europe want to avoid ending up in arrangements which make it difficult for them to process the data they produce themselves and to extract value from it. The intention is not to create systems parallel to the services already offered by incumbent international cloud service providers, but to build something new."[76] As of this writing, the project remains in the planning stage.[77]

Conclusion

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. Facebook, Strava, ToTok, FaceApp and TikTok threaten national security in different ways, but their use of personal data remains underregulated in all three nations. 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 (*what and how*) and not in the governance of data. US policy makers have not addressed the real problem, which is the failure to adequately govern how personal data is used, monetized and protected. Instead, the United States has banned certain apps and adopted investment reviews of foreign firms that want to acquire firms with large troves of personal data. Meanwhile, Canada and Germany see a different national security risk. They 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.

72 See Public Safety Canada (2019).

73 See Federal Ministry of Economic Affairs and Energy, n.d.(a), 3.

74 Ibid.

75 See Meyer (2019).

76 See Weiss (2019).

77 See Federal Ministry of Economic Affairs and Energy, n.d.(b).

Meanwhile, 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. The United States could do so much more to mitigate the threat of misuse of data within its borders and abroad if it adopted a strong personal data protection law. Americans (and the world at large that relies on these data-driven services) need clear rules governing how firms can obtain, monetize and distribute personal data.

The case studies also reveal that even countries such as Germany with strong personal data protection laws must update their approach to regulating the use of personal data. Although the law is new, it has not caught up with technological innovations. Just as we count on social networks to regulate content on their sites, the app market is governed by a few large data giants rather than government officials. Sometimes, as we have seen with ToTok, dangerous applications slip through the cracks. No firm or government should be allowed to sell or provide for free an app for surveillance purposes, even in times of national emergency. In addition, firms should not use apps to gather the personal data of users that is not essential to the proper functioning of such apps. 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 where governments see similar risks in data troves, they are not cooperating on policy solutions. The best place for governments to address this issue is not only at the national level but, given the global nature of the internet, internationally. Trade agreements are currently the only venue to find a multilateral approach to these issues. Trade agreements should be drafted to facilitate the free flow of data while protecting user privacy. Yet the European Union (Germany), Canada and the United States have taken very different approaches to personal data governance in trade agreements. The European Union makes personal data protection a priority before personal data can flow across borders, while the United States and Canada have accepted trade agreements with language establishing only a privacy floor. Such fragmentation could lead to higher costs to data users and producers. Hence nations should cooperate on interoperable language for personal data protection.

In sum, data troves held by governments and firms can present a multitude of security risks. However, policy makers have put forward nationalistic solutions that do not reflect the global nature of the risk. The United States, Canada and Germany should be collaborating to define and mitigate these risks.

Author's Note

The author is grateful to colleagues at the Atlantic Council; James Nelson of George Washington University (GWU), who provided early comments; and the anonymous reviewer who prodded her to think more broadly about the problem of data troves. She also benefited from research assistance from Charlene Burns at GWU and Kailee Hilt at CIGI.

Works Cited

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. Waterloo, ON: CIGI. www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows.

———. 2019. *Data Is a Development Issue*. CIGI Paper No. 223. Waterloo, ON: CIGI. www.cigionline.org/publications/data-development-issue.

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.

Abrams, Martin. 2019. "Privacy and data protection: What's in a name?" IAPP, November 15. https://iapp.org/news/a/privacy-and-data-protection-whats-in-a-name/.

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.

Bailey, Tricia. n.d. "Identity Theft and the Underground Economy." Center for Identity, University of Texas at Austin. https://identity.utexas.edu/id-perspectives/identity-theft-and-the-underground-economy.

Baron Cohen, Sacha. 2019. "Sacha Baron Cohen's Keynote Address at ADL's 2019 Never Is Now Summit on Anti-Semitism and Hate." ADL, November 21. www.adl.org/news/article/sacha-baron-cohens-keynote-address-at-adls-2019-never-is-now-summit-on-anti-semitism.

Barth, Brian. 2019. "Big Tech's Big Defector." *The New Yorker*, December 2. www.newyorker.com/magazine/2019/12/02/big-techs-big-defector.

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.

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.

Bing, Christopher and Joel Schectman. 2019. "Project Raven: Inside the UAE's Secret Hacking Team of American Mercenaries." Reuters, December 21. www.reuters.com/investigates/special-report/usa-spying-raven/.

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/.

Bushatz, Amy. 2015. "Report: Hack of Adultery Site Ashley Madison Exposed Military Emails." Military.com, August 19. www.military.com/daily-news/2015/08/19/report-hack-adultery-site-ashleymadison-exposed-military-emails.html.

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.

Carrière-Swallow, Yan and Vikram Haksar. 2019. "The Economics of Data." *IMFBlog* (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/.

Carter, William A. 2019. "Ensuring Data Security Against Lawful and Unlawful Threats in the Digital Age." Statement before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism. November 5. www.judiciary.senate.gov/imo/media/doc/Carter%20Testimony.pdf.

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.

Cherian, Dona. 2020. "ToTok, internet calling apps in UAE: What we know about the story so far." *Gulf News*, February 24. https://gulfnews.com/photos/news/totok-internet-calling-apps-in-uae-what-we-know-about-the-story-so-far-1.1577260083008?slide=1.

Chesney, Robert. 2019. "Project Raven: What Happens When U.S. Personnel Serve a Foreign Intelligence Agency?" *Lawfare* (blog), February 11. www.lawfareblog.com/project-raven-what-happens-when-us-personnel-serve-foreign-intelligence-agency.

Cimpanu, Catalin. 2019. "Facebook removes propaganda network linked to Russian media group Sputnik." ZDNet, January 17. www.zdnet.com/article/facebook-removes-propaganda-network-linked-to-russian-media-group-sputnik/.

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/.

Connolly, Kate. 2019. "German cyber-attack: man admits massive data breach, say police." *The Guardian*, January 8. www.theguardian.com/world/2019/jan/08/germany-data-breach-man-held-in-suspected-hacking-case.

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/army-recruiters-still-using-tiktok-amid-national-security-probe.html.

———. 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.

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. 2018. *The App Economy in the United States*. August 17. https://actonline.org/wp-content/uploads/Deloitte-The-App-Economy-in-US.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/.

Department of Homeland Security. 2017. *Handbook for Safeguarding Sensitive PII: Privacy Policy Directive 047-01-007*. Revision 3. DHS Privacy Office, December 4. www.dhs.gov/sites/default/files/publications/dhs%20policy%20directive%20047-01-007%20handbook%20for%20safeguarding%20sensitive%20PII%2012-4-2017.pdf.

Dwoskin, Elizabeth. 2019. "Zuckerberg says he'll reorient Facebook toward encryption and privacy." *The Washington Post*, March 6. www.washingtonpost.com/technology/2019/03/06/facebooks-mark-zuckerberg-says-hell-reorient-company-towards-encryption-privacy/.

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

Federal Ministry of Economic Affairs and Energy. n.d.(a). *Project Gaia-X*. www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/das-projekt-gaia-x-executive-summary.pdf?__blob=publicationFile&v=6.

———. n.d.(b). *A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem*. www.bmwi.de/Redaktion/EN/Artikel/Digital-World/data-infrastructure.html.

Fennessy, Caitlin. 2019. *GDPR at One Year: What We Heard from Leading European Regulators*. IAPP, White Paper. March. https://iapp.org/resources/article/gdpr-at-one-year-dpas/.

Fischer, Sara and Scott Rosenberg. 2019. "Government wants access to personal data while it pushes privacy." Axios, August 26. www.axios.com/government-wants-access-to-personal-data-while-it-pushes-privacy-aacc15f1-bbcb-481b-b6ae-278e0f15e678.html.

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/.

Frenkel, Sheera, Nicholas Confessore, Cecilia Kang, Matthew Rosenberg and Jack Nicas. 2018. "Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis." *The New York Times*, November 14. www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html.

Fruhlinger, Josh. 2020. "The OPM hack explained: Bad security practices meet China's Captain America." CSO, February 12. www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

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.

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

Germano, Sara. 2020. "German Court Rules Against Facebook on Data Protection." *The Wall Street Journal*, January 24. www.wsj.com/articles/german-court-rules-against-facebook-on-data-protection-11579891532.

Ghorayshi, Azeen. 2018. "Grindr Will Stop Sharing Users' HIV Data With Other Companies." BuzzFeed News, April 2. www.buzzfeednews.com/article/azeenghorayshi/grindr-stopped-sharing-hiv-status#.qrV4alOQz.

Ghorayshi, Azeen and Sri Ray. 2018. "Grindr Is Letting Other Companies See User HIV Status And Location Data." BuzzFeed News, April 2. www.buzzfeednews.com/article/azeenghorayshi/grindr-hiv-status-privacy.

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

Gilbert, Ben. 2018. "Facebook just published a message for its users: No, you're not the product." April 23. www.businessinsider.com/facebook-advertising-users-as-products-2018-4.

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.

Goode, Lauren. 2018. "Strava users, in midst of privacy problems, are reporting that one of the app's top features has been disabled." The Verge, February 5. www.theverge.com/2018/2/5/16974576/strava-public-segment-feature-disabled-app-privacy-heatmaps.

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/.

Gregoire, Carolyn. 2015. "Ashley Madison Hack Could Have A Devastating Psychological Fallout." Huffington Post, August 20. www.huffpost.com/entry/ashley-madison-hack-psychological-fallout_n_55d4afcee4b07addcb44f5d4.

Hardwick, Tim. 2019. "Apple Pulls Emirati Chat App 'ToTok' From App Store for Allegedly Spying on Users." MacRumors, December 23. www.macrumors.com/2019/12/23/apple-pulls-chat-app-totok-secret-spying-tool/.

Hartzog, Woodrow and Neil Richards. 2020. "Why Europe's GDPR magic will never work in the US." *Wired*, February 20. www.wired.co.uk/article/us-version-gdpr.

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.

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/.

Hungerford, Nancy. 2019. "Chinese theft of trade secrets on the rise, the US Justice Department warns." CNBC, September 22. www.cnbc.com/2019/09/23/chinese-theft-of-trade-secrets-is-on-the-rise-us-doj-warns.html.

Hu, Jane. 2012. "A Little History Of Blackmail." *The Awl*, June 21. www.theawl.com/2012/06/a-little-history-of-blackmail/.

Hutchinson, Andrew. 2019. "Facebook Reaches 2.38 Billion Users, Beats Revenue Estimates in Latest Update." SocialMediaToday, April 24. www.socialmediatoday.com/news/facebook-reaches-238-billion-users-beats-revenue-estimates-in-latest-upda/553403/.

Industry and Security Bureau. 2018. "Review of Controls for Certain Emerging Technologies." Regulations.gov, November 19. www.regulations.gov/document?D=BIS-2018-0024-0001.

———. 2020. "Addition of Software Specially Designed To Automate the Analysis of Geospatial Imagery to the Export Control Classification Number 0Y521 Series." Federal Register, January 6. www.federalregister.gov/documents/2020/01/06/2019-27649/addition-of-software-specially-designed-to-automate-the-analysis-of-geospatial-imagery-to-the-export.

Intelligence Advanced Research Projects Activity. 2011. "Open Source Indicators (OSI)." www.iarpa.gov/index.php/research-programs/osi/baa.

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.

Krebs, Brian. 2015a. "Online Cheating Site AshleyMadison Hacked." Krebs on Security, July 15. https://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/.

———. 2015b. "Extortionists Target Ashley Madison Users." Krebs on Security, August 15. https://krebsonsecurity.com/2015/08/extortionists-target-ashley-madison-users/.

Kulwin, Noah. 2018. "The Internet Apologizes." *Intelligencer*, April 13. https://nymag.com/intelligencer/2018/04/an-apology-for-the-internet-from-the-people-who-built-it.html.

LaForgia, Michael and Gabriel J.X. Dance. 2018. "Facebook gave data access to Chinese firm flagged by US intelligence." *The New York Times*, June 5. www.nytimes.com/2018/06/05/technology/facebook-device-partnerships-china.html.

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

Law360. 2019. "Security Fears Dog DOJ As Foreign Tech Cos. Collect US Data." Law360, October 23. www.law360.com/corporate/articles/1212390/security-fears-dog-doj-as-foreign-tech-cos-collect-us-data.

Le Blond, Josie. 2019. "German politicians' personal data leaked online." *The Guardian*, January 4. www.theguardian.com/world/2019/jan/04/german-politicians-personal-data-hacked-and-posted-online.

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.

Lilley, Kevin. 2015. "20,000 soldiers tapped for Army fitness program's 2nd trial." Army Times, July 27. www.armytimes.com/news/your-army/2015/07/27/20000-soldiers-tapped-for-army-fitness-program-s-2nd-trial/.

Lindsley, Mary. 2019. "Former Facebook Global Policy Expert to Lead Tech Policy Initiative at Duke." Sanford School of Public Policy, Duke University, October 15. https://sanford.duke.edu/articles/former-facebook-global-policy-expert-lead-tech-policy-initiative-duke.

Longo, Matthew. 2020. "Your body is a passport." Politico, January 8. www.politico.eu/article/future-passports-biometric-risk-profiles-the-codes-we-carry/.

Lucas, Edward. 2019. "The Spycraft Revolution." *Foreign Policy*, April 27. https://foreignpolicy.com/2019/04/27/the-spycraft-revolution-espionage-technology/.

Markey, Edward J. and Richard Blumenthal. 2018. Letter from Senators Edward J. Markey and Richard Blumenthal to Zhou Yahui, Interim CEO of Grindr. April 3. www.markey.senate.gov/imo/media/doc/grindr%20letter.pdf.

Mazetti, Mark, Nicole Perlroth and Ronin Bergman. 2019. "It Seemed Like a Popular Chat App. It's Secretly a Spy Tool." *The New York Times*, December 22. www.nytimes.com/2019/12/22/us/politics/totok-app-uae.html?searchResultPosition=3.

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/.

Meschke, Jacob. 2018. "Pentagon Severely Restricts Fitness Trackers After Strava Heatmap Scandal." Bicycling, August 10. www.bicycling.com/news/a22699171/pentagon-geolocation-devices-strava/.

Meyer, David. 2019. "Europe Is Starting to Declare Its Cloud Independence." *Fortune*, October 30. https://fortune.com/2019/10/30/europe-cloud-independence-gaia-x-germany-france/?showAdminBar=true.

Morrison & Foerster LLP. 2020. "Foreign Investment 2020 (Part 5): Final CFIUS Rules Announced." JDSupra, January 17. www.jdsupra.com/legalnews/foreign-investment-2020-part-5-final-88589/.

Narayanan, Arvind. 2019. "How to recognize AI snake oil." Center for Information Technology Policy, Princeton University, November 21. www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf.

National Security Agency Central Security Service. n.d. *Understanding the Threat*. www.nsa.gov/what-we-do/understanding-the-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.

Noyes, Dan. 2020. "The Top 20 Valuable Facebook Statistics — Updated January 2020." https://zephoria.com/top-15-valuable-facebook-statistics/.

O'Connor, Nuala. 2018. "Reforming the U.S. Approach to Data Protection and Privacy." CFR, January 30. www.cfr.org/report/reforming-us-approach-data-protection.

Office of the Director of National Intelligence. 2020. *The National Counterintelligence Strategy of the United States of America 2020–2022*. January 7. www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf.

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.

OPC. 2014. *Data Brokers: A Look at the Canadian and American Landscape.* September. www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/db_201409/.

———. 2019a. *Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia.* PIPEDA Report of Findings #2019-002, April 25. www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/.

———. 2019b. *2018-2019 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act*. December 10. www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/.

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.

Papamiltiadis, Konstantinos. 2019. "Changes to Groups API Access." *Facebook for Developers* (blog), November 5. https://developers.facebook.com/blog/post/2019/11/05/changes-groups-api-access/.

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/.

Perper, Rosie. "Facebook could be fined up to $1.63 billion for a massive breach which may have violated EU privacy laws." Business Insider, October 1. www.businessinsider.in/facebook-could-be-fined-up-to-1-63-billion-for-a-massive-breach-which-may-have-violated-eu-privacy-laws/articleshow/66021864.cms.

PR Newswire. 2016. "Avid Life Media Rebrands as ruby — Officially Drops Ashley Madison Life is Short. Have an Affair. Tagline." PR Newswire, July 12. www.prnewswire.com/news-releases/avid-life-media-rebrands-as-ruby---officially-drops-ashley-madison-life-is-short-have-an-affair-tagline-300297105.html.

Public Safety Canada. 2019. *Economic-based Threats to National Security*. November 20. www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/trnstn-bndrs/20191120/030/index-en.aspx.

Quarles, James. 2018. "A Letter to the Strava Community." *Strava Press* (blog), January 29. https://blog.strava.com/press/a-letter-to-the-strava-community/.

Ram, Aliya and Madhumita Murgia. 2019. "Data brokers: regulators try to rein in the 'privacy deathstars.'" *Financial Times*, January 7. www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521; www.ciodive.com/news/report-gdpr-regulators-digging-into-data-brokers/545682/.

Rempfer, Kyle, Shawn Snow and Howard Altman. 2020. "Families of deployed paratroopers received 'menacing' messages, warned to double-check social media settings." MilitaryTimes, January 15. www.militarytimes.com/flashpoints/2020/01/15/family-members-of-deployed-paratroopers-receiving-menacing-messages-warned-to-double-check-social-media-settings/.

Reuters. 2012. "Zuckerberg's letter to investors." Reuters, February 1. www.reuters.com/article/us-facebook-letter-idUSTRE8102MT20120201.

———. 2015. "Canada's capital is a hotspot for Ashley Madison users, now hacking victims." *The Guardian*, July 21. www.theguardian.com/world/2015/jul/21/canada-ottawa-ashley-madison-hacking.

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

Romm, Tony. 2018. "Facebook granted devices from Huawei, a Chinese telecom firm, special access to social data." *The Washington Post*, June 5. www.washingtonpost.com/news/the-switch/wp/2018/06/05/facebook-granted-devices-from-huawei-a-chinese-telecom-firm-special-access-to-social-data/?utm_term=.3a368bc308bd.

Rosenberg, Jacob. 2019. "The Trump Administration Apparently Considers Grindr a National Security Threat. What Is Going On?" Mother Jones, April 4. www.motherjones.com/politics/2019/04/the-trump-administration-apparently-considers-grindr-a-national-security-threat-what-is-going-on/.

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.

Sanders, James. 2018. "US intelligence chiefs say Huawei, ZTE products pose national security risk." TechRepublic, February 15. www.techrepublic.com/article/us-intelligence-chiefs-say-huawei-zte-products-pose-national-security-risk/.

Sanders, James and Dan Patterson. 2019. "Facebook data privacy scandal: A cheat sheet." Tech Republic, July 24. www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/.

Schumer, Charles. 2019. Letter from Senator Charles Schumer to Ryan McCarthy, Secretary of the Army. November 7. www.documentcloud.org/documents/6546494-20191107-SECARMY-TikTok.html.

Science Daily. 2019. "National security." www.sciencedaily.com/terms/national_security.htm.

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/.

Select Committee on Intelligence. n.d. *Report of the Select Committee on Intelligence, United States Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*. vol. 2. www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

Silverstein, Richard. 2019. "Dark Matter, Leading UAE Hacking Firm, Entices IDF Cyberwar Veterans at $1-Million a Pop, Israeli Media Report Censored." *Tikun Olam* (blog), October 29. www.richardsilverstein.com/2019/10/29/dark-matter-leading-uae-hacking-firm-recruits-idf-cyberwar-veterans-at-million-dollar-salaries/.

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, Adam Oliver. 2019. "Revealed: Secretive UAE cybersecurity firm with a history of spying on dissidents is operating in Finland." *Helsinki Times*, February 3. 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.

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/.

Standing Committee on Public Safety and National Security. 2019a. *Evidence* (Andrew Clement, professor emeritus, Faculty of Information, University of Toronto). 1st sess., 42nd Parliament. www.ourcommons.ca/DocumentViewer/en/42-1/secu/meeting-152/evidence.

———. 2019b. *Cybersecurity in the Financial Sector as a National Security Issue*. 1st sess., 42nd Parliament. www.ourcommons.ca/Content/Committee/421/SECU/Reports/RP10589448/securp38/securp38-e.pdf.

Sternstein, Aliya and Jack Moore. 2015. "Timeline: What We Know About the OPM Breach." Nextgov, June 26. www.nextgov.com/cybersecurity/2015/06/timeline-what-we-know-about-opm-breach/115603/.

Stone Fish, Isaac. 2019. "China Has Access to Grindr Activity. We Should All Be Worried." *The Washington Post*, April 9. www.washingtonpost.com/opinions/2019/04/09/why-we-cant-leave-grindr-under-chinese-control/.

Strawbridge, James. 2018. "Vermont Publishes New Guidance on Law Regulating 'Data Brokers.'" Inside Privacy, December 21. www.insideprivacy.com/data-privacy/vermont-publishes-new-guidance-on-law-regulating-data-brokers/.

The 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.

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.

Treasury Board of Canada Secretariat. 2018a. *IT Policy Implementation Notice (ITPIN)*. March 13. www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/direction-electronic-data-residency.html.

———. 2018b. *Government of Canada White Paper: Data Sovereignty and Public Cloud*. June 25. www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/gc-white-paper-data-sovereignty-public-cloud.html.

Tucker, Patrick. 2015. "Meet the Man Reinventing CIA for the Big Data Era." Defense One, October 1. www.defenseone.com/technology/2015/10/meet-man-reinventing-cia-big-data-era/122453/.

UNCTAD. 2019. *Data Protection and Privacy Legislation Worldwide*. https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

Valentino-DeVries, Jennifer, Natasha Singer, Michael H. Keller and Aaron Krolik. 2018. "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret." *The New York Times*, December 10. www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

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.

Weiss, Andreas. 2019. "GAIA-X; Growing a Vibrant European Ecosystem." dotmagazine, November. www.dotmagazine.online/issues/on-the-edge-building-the-foundations-for-the-future/gaia-x-a-vibrant-european-ecosystem.

White House. 2019. "Executive Order on Securing the Information and Communications Technology and Services Supply Chain." May 15. www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

World Economic Forum. 2011. *Personal Data: The Emergence of a New Asset Class.* February 17. www.weforum.org/reports/personal-data-emergence-new-asset-class.

Ziv, Amitai. 2019. "Mysterious UAE Cyber Firm Luring ex-Israeli Intel Officers With Astronomical Salaries." *Haaretz*, October 16. https://outline.com/fqUvjM.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

@cigionline