YOUR DATA AS A WEAPON: HOW TIKTOK CAPTURES A SECURITY CRISIS

Christopher Waters*

I. Introduction

In 1890, Samuel Warren and Louis Brandeis published a law review piece which many refer to as "The Right to be Let Alone," a title of intense relevance over one-hundred years later.[1] Privacy can act as the last form of control an individual has against social groups, companies, or governments. As suggested by a litany of acclaimed scholars, privacy is at the core of personal autonomy. Emphasizing this connection between privacy and autonomy, in *The Right of the People*, Justice Douglas stated, "much of this liberty of which we boast comes down to the right of privacy."[2] However, privacy is at risk of erosion due to a variety of causes. With the advent of the digital age in which individuals, corporations, and governments have unfettered communication and access to information, the degradation of this deeply inherent right has increased.

The globe has reached a period of unprecedented connectivity by nearly every measure. Trade, information-sharing, and espionage are all supercharged by the digital revolution. With the Internet, individual privacy hangs in the balance, and both individuals and states should be concerned. Personal data has become a product unto itself, much like how tangible products can be used as currency, tools, or weapons, so too can an individual's information.

This Note analyzes critical perspectives on data through an international security lens. First, it introduces basic organizations

---

* Syracuse University College of Law, J.D. Candidate, Class of 2022. The author extends his thanks to his family for their loving support during the most rigorous portion of his young life. Further, he offers his sincerest thanks to Professor Laurie Hobart for not only her advisement and wealth of knowledge on this Note, but her ability to encourage him to achieve successes he never thought possible.

[1] Louis Brandeis & Samuel Warren, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

[2] WILLIAM DOUGLAS, THE RIGHT OF THE PEOPLE 94-113 (1958).

and trends which handle personal data and cybersecurity concerns. Directly following, this Note discusses the associated international security concerns which are presented within a case study on TikTok. TikTok is a Chinese online application which is critiqued for its practices concerning personal data, yet it is currently exploding with global popularity. Furthermore, there is a discussion of existing government responses and international reactions to data privacy. Finally, this Note states that action is needed to protect personal data on a variety of harmful applications. It could be an international agreement, a cohesive response by the United States, or a restructuring of cyber-focused entities. This Note proposes that if not for moral, legal, or commercial reasons, the country should protect private data out of concern for its security.

II. EXISTING RESPONSES AND TRENDS

A. CURRENT ENTITIES AND FRAMEWORKS

Due to the rapid development of electronic devices and Internet access, the creation of a regulatory organization as well as responses from Washington D.C. and the international community became necessary. There is a decentralized network of entities, regarding internet and global application matters. This issue with internet data regulation might occur because of the web's disregard of clear lines between public and private spaces, conflict and peace, and unfettered connectivity with liberty erosion.[3]

Nevertheless, entities and agreements were created both in the United States and abroad to address issues in cyberspace. The U.S. has a network of roughly twenty agencies with missions dedicated to tackling cyber threats alongside a variety of private organizations.[4] Existing branches, such as the Federal Bureau of Investigations ("FBI"), Department of Homeland Security ("DHS"), and even the Federal Trade Commission ("FTC"), all have offices

---

[3] *See* ROGER C. MOLANDER ET AL., STRATEGIC INFORMATION WARFARE: A NEW FACE OF WAR 19 (RAND Corporation ed., 1996).

[4] Michael Garcia & Mieke Eoyang, *A Roadmap For Tackling Cybercrime*, LAWFARE (Dec. 10, 2020), *available at* https://www.lawfareblog.com/road-map-tackling-cybercrime (last visited Nov. 9, 2021).

and entities for data security.[5] Yet another is the Cybersecurity and Infrastructure Security Agency ("CISA") which functions as the U.S.' risk advisor not only for the public but also the private sector.

Additionally, there is the United States Cyber Command which was established in 2009 but elevated to a Unified Combatant Command in 2018.[6] This entity functions to centralize cyberspace operations, resources, and strengthens Department of Defense ("DoD") cyberspace potential.[7] It does so through "dual hat authority," in which one individual would direct the National Security Agency through Title 50 authorities while also directing Cyber Command under Title 10 authorities.[8] This arrangement was made in the hopes of resolving conflicts between intelligence and military cyber operations while also allowing Cyber Command to mature as an organization.[9]

Although each agency has an individual and tailored mission, there is no clear federal framework establishing liability for compromises in cyberspace.[10] Moreover, few, if any, of these centers on individuals' privacy. This is not to say that a citizen's privacy is never considered. The Privacy and Civil Liberties Oversight Board was created to restrain wanton intelligence collection and to advise the executive branch on privacy concerns impacted by legislation and policies adopted in the fight again

---

[5] Justine Brown, *5 Federal Agencies with a Role in Ensuring Enterprise Cybersecurity,* CIODIVE (Aug. 17, 2016), *available at* https://www.ciodive.com/news/5-federal-agencies-with-a-role-in-ensuring-enterprise-cybersecurity/424557/ (last visited Nov. 9, 2021).

[6] Statement by President Donald J. Trump on the Elevation of Cyber Command, OFF. OF THE PRESS SEC'Y (Aug. 18, 2017), *available at* https://trumpwhitehouse.archives.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/ (last visited Nov. 9, 2021).

[7] *Id.*

[8] Erica D. Borghard, *Time to End Dual Hat?*, COUNCIL ON FOREIGN REL. (Feb. 3, 2021), *available at* https://www.cfr.org/blog/time-end-dual-hat (last visited Nov. 9, 2021).

[9] *Id.*

[10] *See* LYLE J. MORRIS ET AL., GAINING COMPETITIVE ADVANTAGE IN THE GRAY ZONE 140-43 (RAND CORP., 2019).

terrorism.[11] Further, offices or individuals dedicated to advising on privacy are not uncommon. Look to CISA's Office of Privacy which reports to the Director of CISA and ensures compliance with existing privacy policies.[12] Indeed, efforts to ensure privacy protection have been made, but these are largely self-monitoring mechanisms and scarcely touch the private industry which is a source of major data privacy concerns.[13]

To complicate an already vast network of U.S. federal entities, there are also private organizations which act in a variety of capacities such as information sharing, security certifications, and research into security practices. Many of these organizations have international impact, such as the Information Systems Security Association ("ISSA"), a not-for-profit dedicated to providing and sharing knowledge on risks in cyberspace and raising security issues to the public.[14] Within the private realm also sits the Information Systems Audit and Control Association ("ISACA"), which educates professionals and their companies around the world on information security, privacy issues, and the benefits of information technology.[15] While these entities provide meaningful research and expertise to government bodies and private entities, they cannot by themselves enact enforceable laws on an international or even on a state level. That power is left to international governmental organizations.

Our last consideration of existing responses is through a purely international lens. International conflict, commerce, and diplomacy all create potential for data which international governmental organizations have accounted for in varying capacities. For example, Article XXI of the General Agreement on Tariffs and

---

[11] *Privacy and Civil Liberties Oversight Board*, FED. REG., *available at* https://www.federalregister.gov/agencies/privacy-and-civil-liberties-oversight-board (last visited Nov. 9, 2021).

[12] *CISA Office of Privacy*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, *available at* https://www.cisa.gov/privacy (last visited Nov. 9, 2021).

[13] *See Id.*

[14] *Developing and Connecting Cybersecurity Leaders Globally*, INFO. SYS. SEC. ADMIN., *available at* https://www.issa.org/about-issa/ (last visited Oct. 19, 2021).

[15] *Purpose and Promise*, INFO. SYS. AUDIT & CONTROL ASS'N, *available at* https://www.isaca.org/why-isaca/about-us/purpose-and-strategy (last visited Nov. 9, 2021).

Trade ("GATT") contemplates a security exception, in which countries can refuse to furnish information they deem necessary to their security, a massive potential snag for information sharing in an interconnected world.[16] For many nations, the global supply chain, ever increasing in length and complexity, represents a variety of potential data breaches. In response, the Department of Commerce's National Institute of Standards and Technology ("NIST") has created a framework for all businesses to maintain better cyber practices.[17] While the tool is entirely voluntary, it provides corporations with guidance and information in managing privacy risks.

International trade and economic stability can be easily disrupted by cyberthreats or loss of data integrity – both of which can undermine countries' confidence in establishing complex trade deals and citizens' confidence in the international liberal order. This has real impact on global governance. A letter to the United Nations General Assembly ("UN") on the International Code of Conduct for Information Security in 2015 emphasized the importance of an untouched, non-leverageable global information chain.[18] This exemplifies how the issue of data security is growing on the global political stage. It is the opinion of many states that their sovereign power includes the capacity to act unilaterally in cyber and information contexts.

Within states' discussions on existing methods of handling data, the overarching theme is increasing governance or at least awareness of individuals' data rights rather than lackadaisical treatment. Whether it be in a bilateral agreement, a free trade agreement ("FTA"), an Organization for Economic Cooperation ("OECD") promulgation, or new drafts to the U.N. General

---

[16] *Article XXI Security Exceptions*, WORLD TRADE ORG. (n.d.), *available at* https://www.wto.org/english/res_e/booksp_e/gatt_ai_e/art21_e.pdf (last visited Nov. 9, 2021).

[17] *NIST Privacy Framework*, NAT'L INST. OF STANDARDS & TECH. (Jan. 16, 2020), *available at* https://www.nist.gov/privacy-0 (last visited Nov. 9, 2021).

[18] U.N. General Assembly, *Developments in the field of information and telecommunications in the context of information security*, U.N.G.A. (Jan. 9, 2015), *available at* https://digitallibrary.un.org/record/786846/files/A_69_723-EN.pdf (last visited Nov. 9, 2021).

Assembly, it appears that the discussion on private data's vulnerability is increasingly prevalent.

B. ESCALATING SECURITY CONCERNS

Given the lack of a cohesive response from the United States, and the largely fragmented approach adopted on the international stage, one would imagine potential misuse of personal data is not immense. Indeed, private data must be of little use to states acting in cyberspace given that only a few state governments have promulgated protections. Yet nothing could be further from reality, as this piece will demonstrate that there are a staggering number of political uses for personal data, and cyberspace has quickly become a playing field for the world's superpowers.

Simply look to the National Security Commission's Final Report on artificial intelligence in cyberspace, which establishes that our competitors use disinformation to sow discord, surveillance to maintain domestic control, and cyber theft to steal developing technologies.[19] Private data has implications in all these areas, furnishing useful information to adversaries on how to tailor their campaigns in cyberspace. Given this trend, the common idea of data needs readjusting.

First, it is best to reimagine data as a concrete resource with a variety of uses rather than mere statistics and measurements. It has particularized and diverse applications. A malicious actor could learn an individual's geographic location, relative age, occupation, education, political affiliation, and even their preferred brands simply by getting that individual to accept a friend request on Facebook. Then the actor could tailor what that individual views on that platform or even outsource that information to an entity with grander goals.

Few other instances could exemplify this perspective better than the Cambridge Analytica scandal. The analytics company publicly stated that it used demographic polling and microtargeting

---

[19] Final Report on Artificial Intelligence, March 2021, NAT'L SEC. COMM'N, *available at* https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf (last visited Nov. 9, 2021).

to understand voters' internal driving behavior. But in reality, Cambridge Analytica built profiles on hundreds of millions of voters, then influenced their voting behavior using tailored disinformation.[20] To Western democratic governments this revealed how quickly electorates can be targeted and socially engineered by online entities using only their private data.

Cambridge Analytica represented a massive shift in how an individual's data can have value in a security context, even drawing a response from the U.S. government in the form of the Voter Privacy Act.[21] The act notes that data has dangerous potential in the political sphere: "[o]ne U.S. based search engine advertises its ability to track hundreds of categories of data about specific individuals including age, gender, occupation, income level, sexual orientation . . . religion . . . and support for social issues . . ."[22] This demographic data collected from that individual is then broadcasted or sold to other companies both domestic and foreign. Key here is the data's near limitless uses in the hands of a malicious actor, all without the individual's choice or knowledge. Indeed, personal data can be both a political commodity and a security risk when considering the implications in free elections, media consumption, and radicalization. The Act defines covered entities, personal information, and online targeting, then outlines how a voter can request to have their collected information proffered, erased, or protected from transfer.[23] Unfortunately, the Voter Privacy Act has yet to be codified as of January 2021.

However, this is a view of personal data's use in an open democracy, namely the United States. The treatment personal data receives in the security context changes between governments. Such treatment often reflects the norms of the given state; in the U.S. it is often collected for commercial purposes or with hopes to disrupt the electorate, whereas in China's personal data is surveilled for

---

[20] Patrick Day, *Cambridge Analytica and Voter Privacy*, 4 GEO. L. TECH. REV. 583, 585-6 (2020).
[21] *Id.* at 590.
[22] Voter Privacy Act of 2019, S. 2398, 116 Cong. §2(3) (2019).
[23] *Id.* at §351-4.

domestic security concerns beyond what even a post-9/11 United States would consider permissible.

China's newest Cybersecurity and National Security Laws regulate data in its critical infrastructure sectors, defined broadly, but also demands that collected data be stored in mainland China.[24] While this raises concerns for trading partners, it also reflects the Chinese Communist Party's ("CCP") domination over personal information for the sake of state security. Further, with every passing year the CCP intensifies its cyber theft campaigns, and with the advent of artificial intelligence in cyberspace, their frequency and impact will skyrocket.[25] China has a known policy of exploiting intellectual property laws in the U.S. to close the gaps between our dual-use technologies and their own.[26]

Lastly, a norm under Chinese authority is censorship, culminating in what is known as the "Great Firewall." China's Cyberspace Administration broadly defines unacceptable content and will ban entire apps such as Facebook or language deemed harmful to the state.[27] The authoritarian CCP has reckoned with the risks personal data might pose to the regime from outside their borders as well as the risks it poses from any domestic dissenters. Thus far, we have a liberal democracy's slow response and an authoritarian's aggressive response to private data risks. With luck, Europe provides a moderate viewpoint.

Both the U.S. and China's privacy laws can be contrasted with how the European Union ("EU") champions individual privacy from a place of concern for both state security and respect for the individual. The main piece of legislation in the EU is the General Data Protection Regulation ("GDPR") which is designed to give

---

[24] Chris Mirasola, *An Update on Chinese Cybersecurity and the WTO*, LAWFARE (March 2, 2018), *available at* https://www.lawfareblog.com/update-chinese-cybersecurity-and-wto (last visited Nov. 9, 2021).

[25] *Final Report on Artificial Intelligence*, NAT'L SEC. COMM'N (Mar. 2021), *available at* https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf (last visited Nov. 9, 2021).

[26] *Id.* at 12.

[27] David Bandurski, *A Brief Experiment in an Open Chinese Web*, BROOKINGS INST. (Nov. 12, 2020), *available at* https://www.brookings.edu/techstream/a-brief-experiment-in-a-more-open-chinese-web/ (last visited Nov. 9, 2021).

citizens more control on how their data is collected and used. It also bars the transfer of personal data outside the European Economic Area unless the third country's regulations are deemed adequate by the European Commission.[28] This treatment demonstrates the EU's attention to personal and consumer rights, both to be protected by the state in the absence of a global agreement. The European situation demonstrates faith in government regulation, adherence to the rights of the individual, and a reckoning with modern security issues.

C. TECHNICAL CONSIDERATIONS

Concluding this introduction, a discussion of basic practices in data collection and storage is warranted. As previously touched upon, personal data is an interest to both the state and private industry – it constitutes a potential security leverage or an insight into the behavior of citizens. To private companies, personal data is an insight into what consumers want, how quickly, and at what price they see as acceptable. While state governments have a stake in where that data is stored with multiple motivations: their own security, their competition against adversaries, and protecting their citizens' individual rights.

Our knowledge of other state practices is limited, but the National Security Agency ("NSA") in the U.S. gives insight into technical government practices. The PRISM program run by the NSA finds legal footing in several laws: Section 702 of the Foreign Intelligence Surveillance Act, the now restricted Section 215 of the Patriot Act, and guidance provided by Foreign Intelligence Surveillance Courts.[29] But restrictions the government faces change by method of collection, person, and type of data being collected. Nevertheless, for the collection of telephone and Internet metadata, at least one end of the data transfer must generally be outside the U.S.[30] How long this data can be stored also depends on its source, for example,

---

[28] *UK: Understanding the Full Impact of Brexit on UK: Data Flows,* DLA PIPER (Sept. 23, 2019), *available at* https://blogs.dlapiper.com/privacymatters/uk-gdpr-brexit-flowchart/ (last visited Nov. 9, 2021).

[29] *National Security Agency Surveillance*, AM. C.L. UNION, *available at* https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance (last visited Nov. 9, 2021).

[30] *Id.*

telephone metadata is small in terms of needed storage space but can be stored for five years.[31]

The NSA stores collected private data in a two billion dollar, one million square foot complex in Utah that can store data, break codes, and probe the dark web.[32] It centralizes collected data from NSA headquarters, overseas posts, and other telecom facilities in amounts beyond common parlance, such as the immense "yottabyte."[25] Clearly, the U.S. does have the capacity and budget to act.

For the private industry, storage of private data must comport with domestic laws both where it is stored and from whom it is collected. Companies have immense motivation to collect and store personal data when considering the commercial advantages of knowing search histories, locations, connections, wish lists, purchases, and more. Yet, private storage practices are not overly diverse, with more than half of the globe's cloud storage used by four corporations: Amazon, Microsoft, IBM, and Google.[26] Given the wealth and international scope of these Internet magnates, it is relatively easy for companies to duplicate user data onto a server thousands of miles from that user.[27] This has caused a surge in calls for data residency laws, which would compel companies to store data within national territory.[28] This is demonstrated in the European Union's cogent GDPR, or even China's Great Firewall mentioned earlier.

---

[31] *What You Need to Know About the NSA's Surveillance Programs*, PRO PUBLICA (Aug. 5, 2013), *available at* https://www.propublica.org/article/nsa-data-collection-faq (last visited Nov. 9, 2021).

[32] James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED (Mar. 15, 2012), *available at* https://www.wired.com/2012/03/ff-nsadatacenter/ (last visited Nov. 9, 2021).

[25] *Id.* (A yottabyte is 10^{24} bytes of data. While the common gigabyte has one billion bytes of data, a yottabyte is one septillion bytes of data.)

[26] Rob Crossley, *Where in the world is my data and how secure is it?*, BBC (Aug. 9, 2016), *available at* https://www.bbc.com/news/business-36854292 (last visited Nov. 9, 2021).

[27] *Id.*

[28] Lothar Determann, *How data residency laws can harm privacy*, WORLD ECON. F. (Jun. 9, 2020), *available at* https://www.weforum.org/agenda/2020/06/where-data-is-stored-could-impact-privacy-commerce-and-even-national-security-here-s-why/ (last visited Nov. 9, 2021).

However, even data residency laws allow for international transfers if companies can meet the standards for adequate security. Even more, some suggest that government agencies have more to gain from data residency laws than individuals, and some treaties such as the Trans-Pacific Partnership Agreement specifically outlaw adopting data residency regulations.[29] This regional free trade agreement between the U.S. and eleven other countries requires participants to develop a legal framework on data that is compatible with the other participants – with the overarching goal of easy cross-border data transfers.[30] This is affirmed in Article 14.13 of the treaty which prevents member countries from requiring companies to store data within their territory.[31] The debate on local control versus an open international system continues; but given the hesitancy towards a global regulatory scheme local data residency laws and state driven private data regulation seems more likely.

After covering existing organizations and frameworks, the variety of applications private data has, and actual processes of storing data, we have a foundation moving forward. In sum, there are a variety of existing organizations and frameworks and a similar variety of applications for private data. Further, the U.S. is faced with increased pressure from allies to join the effort in privacy protection and competitors who view data as leverage.

From here this Note continues into dire security concerns exemplified in a case study, a more in-depth analysis of regulatory responses, concluding with possible options on how to protect personal data with respect to state security.

---

[29] *Id.*

[30] *The Trans-Pacific Partnership's Take on Personal Data*, TAYLOR WESSING GLOB. DATA HUB, (Dec. 2015), *available at* https://globaldatahub.taylorwessing.com/article/the-trans-pacific-partnerships-take-on-personal-data (last visited Nov. 9, 2021).

[39] *Id.*

II. Security Threats Through Data: A Case Study

The previous section introduced the idea that an individual's data can be seemingly harmless, yet when harvested can be used maliciously by both companies and governments alike. Similarly, at first glance an app filled with gleeful young adults dancing and creating trends may seem like nothing more than the newest hit online platform. Indeed, individuals can simply create memes, participate in political discussions, reference pop culture, or dancing away on TikTok. Yet by nearly every measure this video sharing social app is simply staggering and, in some cases, not in a positive way.

Created by the Chinese company ByteDance in 2016, the TikTok has had a meteoric rise since 2019 with over two billion downloads worldwide.[32] Its popularity here in the U.S. is also alarming when broken down by demographics. By March 2021, roughly twenty-five percent of its American accounts were held by ten to nineteen year olds.[33] Indeed, as reported in *Business Insider*, many of the world's most popular TikTok "influencers" are as young as seventeen, and few are older than thirty.[34] This means that there are millions of impressionable users with unfettered access to a range of content; the most popular of which can be created by users just as young.

---

[40] Brandon Doyle, *TikTok Statistics – Updated Sep 2021*, WALLAROO MEDIA (Sep. 27, 2021), *available at* https://wallaroomedia.com/blog/social-media/tiktok-statistics/#:~:text=Total%20App%20Downloads%20%E2%80%93%20The%20TikTok,Tower%200n%20April%2029%2C%202020 (last visited Nov. 9, 2021).

[41] J. Clement, *Distribution of TikTok Users in the United States as of March 2021, by age group*, STATISTA (Apr. 2021), *available at* https://www.statista.com/statistics/1095186/tiktok-us-users-age/ (last visited Nov. 9, 2021).

[42] *See* Paige Leskin & Palmer Haasch, *Charli D'Amelio has taken over as TikTok's biggest star. These are the Top 40 Most Popular Creators on the Viral Video App*, BUS. INSIDER (Dec. 24, 2020), *available at* https://www.businessinsider.com/tiktok-most-popular-stars-gen-z-influencers-social-media-app-2019-6 (last visited Nov. 9, 2021).

Without discussing the discourse on content and age, which merits a separate discussion in its own right, these numbers alone certainly create a security risk. The massively influential content creators themselves are likely unaware of how their personal data and accounts are being used, and their audiences – likely just as young or younger, also are unaware of how much of their information ByteDance collects, and what can be done with that information. The amount of both legal and technological literacy required to parse TikTok's user agreement and collection practices simply cannot be expected of anyone under the age of eighteen or even an adult user.

Against the backdrop of its sheer popularity, TikTok also collects users' data in staggering amounts, all emphasized when discussed in a national security context. American citizens can now act as sources of data for an adversary: an unaware statesperson who uses TikTok may be the target of cyber espionage, the lay user may act as a test-run for CCP talking points, or the CCP may simply compel ByteDance to furnish information from users in the military.

This scenario is not conjecture, in its Final Report on AI the National Security Commission stated outright, "Adversaries will combine widely available commercial data with data acquired illicitly . . . to track, manipulate, and coerce individuals."[35] The report goes on to say that the government must start viewing citizens' data as a national security asset as adversaries use it to map individuals and sociopolitical networks, predict behaviors, and illicit responses to online stimuli.[36] Indeed, TikTok can act as an excellent case study into how an individual's data can have broad implications in international security dilemmas.

A. JUDICIAL RESPONSE

Since the Cambridge Analytica Scandal, lawmakers and civil rights activists have placed big tech companies under increasing scrutiny, and ByteDance is no exception. The Chinese tech company owns

---

[43] *Final Report on Artificial Intelligence* 47, NAT'L SEC. COMM'N ON ARTIFICIAL INTELLIGENCE (Mar. 2021), *available at* https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf (last visited Nov. 9, 2021).
[44] *Id.* at 50.

TikTok as well as the Chinese version of the app "Douyin," and in mid-2020 it faced several lawsuits alleging unfair data collection on an unprecedented level. In the U.S. District Court for the Northern District of California, Misty Hong, a student, sued the company for allegedly creating a dossier of her private information, which even included biometric data such as fingerprints and facial recognition.[37]

In the face of legal backlash, ByteDance has assured users it does not transfer any collected data to its servers in China[38] Hong's case has been consolidated into one class action lawsuit and an FTC investigation into whether ByteDance collected information on children under the age of thirteen, which would violate U.S. privacy law.[39] This legal activity propelled TikTok into national headlines and created demand for a legislative response on Capitol Hill, as several testimonies and a Department of Treasury Committee on Foreign Investment in the United States ("CFIUS") investigation would demonstrate.

B. CONGRESSIONAL RESPONSE

Indeed, as lawsuits began to form, the political branches began to take great interest in TikTok's collection activity. By June 2020, U.S. Senators began to request a Department of Justice ("DoJ") inquiry into ByteDance's collection processes, even going so far as to state that Chinese tech firms are notorious for operating under

---

[45] Katie Paul, *TikTok Accused in California Lawsuit of Sending User Data to China*, REUTERS (Dec. 2, 2019), *available at* https://www.reuters.com/article/us-usa-tiktok-lawsuit/tiktok-accused-in-california-lawsuit-of-sending-user-data-to-china-idUSKBN1Y708Q (last visited Nov. 9, 2021).

[46] *Id.*

[47] William Reinsch, Jack Caporal, Patrick Samuell, Isabella Frymoyer, *TikTok is Running Out of Time: Understanding the CFIUS Decision and Its Implications*, CTR. FOR STRATEGIC & INT'L STUD. (Sept. 2, 2020), *available at* https://www.csis.org/analysis/tiktok-running-out-time-understanding-cfius-decision-and-its-implications (last visited Nov. 9, 2021).

draconian intelligence laws.[40] This culminated in a CFIUS investigation into ByteDance's ownership.[41]

CFIUS is an interagency group derived from Section 721 of the Defense Production Act of 1950, that reviews mergers, acquisitions, and foreign investments alleged to be a concern to national security.[42] Using the 2018 Foreign Investment Risk Review Modernization Act, the committee can, and did, determine that ByteDance's ownership and practices represented a threat to American security. The upshot of this decision by CFIUS was that that it gave the White House justification for a potential ban of the TikTok unless ownership of company was handed over to an American company.[43] There has been ample testimony and outcries from lawmakers in Congress. These outcries were shown through the "No TikTok on Government Devices Act", passed in August 2020.[44] Per the CFIUS recommendation, ByteDance is in negotiation to retain a minority stake in TikTok while releasing ownership to bidding U.S. companies; including Oracle, Walmart, and several venture capital firms.[45]

C. EXECUTIVE RESPONSE

These Congressional and CFIUS actions play out in the background of actions taken by the White House, which have mostly failed in

---

[40] Khorrri Atkinson, *Sens. Demand DOJ Open Probe Into Zoom, TikTok China Ties*, LAW360 (Jul. 30, 2020), *available at* https://plus.lexis.com/document/?pdmfid=1530671&crid=90dfdbcf-077e-4b1c-9886-8194fe92d8f6&pddocfullpath=%2Fshared%2Fdocument%2Flegalnews%2Furn%3AcontentItem%3A60GF-MG71- JGPY-X004-00000-00&pdcontentcomponentid=122080&pdteaserkey=&pdislpamode=false&pdworkfolderlocatorid=NOT_SAVED_IN_WORKFOLDER&ecomp=hf4hk&earg=sr0&prid=00c0ed67-e38a-426c-afde-a455c0c5ca3e (last visited Nov. 9, 2021).

[41] Reinsch, *supra* note 47.

[42] Treas. Reg. § 721 (as amended in 2018).

[43] Reinsch, *supra* note 47.

[44] No TikTok on Government Devices Act, S. 3455, 116th Cong. (2020)

[45] Dan Primack, *TikTok Gets More Time, Again*, AXIOS (Dec. 5, 2020), https://www.axios.com/tiktok-bytedance-deadline-national-security-cfius-574ba5d0-cb46-4a1e-9f27-99354a12d6b9.html (last visited Nov. 9, 2021).

federal courts. In May 2020, President Donald Trump invoked his authority under International Emergency Economic Powers Act ("IEEPA"), declaring a national emergency concerning foreign technology companies threatening U.S. security.[46] In doing so, President Trump identified TikTok as a threat to the nation's security and ordered divestment in August 2020 through CFIUS and identification of prohibited transactions by the Secretary of Commerce. These directions were completed in August 2020 through Executive Order 13942.[47]

By late September 2020, the D.C. District Court issued a preliminary injunction on behalf of ByteDance. One month later in another case between angered TikTok users and the Trump Administration, the Eastern District Court of Pennsylvania issued another injunction on behalf of the plaintiffs. The court held that the IEEPA was violated by an attempt to regulate informational materials which would harm plaintiffs.[48] Indeed, from September to December of 2020 the Trump Administration's actions against TikTok have yielded poor results.

D. BYTEDANCE AND BEIJING

In the beginning of this section, the discussion was of a popular app that collected users' data. Why is such an app such a concern to U.S. lawmakers, the White House, and federal courts, when Facebook, Instagram, and Google often do the same? Assuredly, given the significant government response, one might consider what data is being collected that would merit such a response given that personal data is collected by a variety of other apps, companies, and even the NSA post-9/11.

However, the private data which TikTok collects from users is staggering even when compared to mainstream competitors such as Instagram, Facebook, or Twitter. A user's location, device information, cookies, even clipboard information – which could include passwords, are all accessible to ByteDance.[49] It is crucial to

---

[46] TikTok, Inc. v. Trump, 507 F. Supp. 3d 92 (D.D.C. 2020).
[47] *Id.*
[48] Maryland v. Trump, 498 F. Supp. 3d 624 (E.D. Pa. 2020).
[49] *Id.*

distinguish TikTok's collection from other applications, such as Facebook and YouTube, whose practices are arguably reprehensible as well.

The distinction continues with ByteDance's aggressive and novel collection techniques. TikTok faced scrutiny for dodging a Google Android privacy layer by collecting individual device information in MAC addresses.[50] Even more, the app creates a new encryption with every update, meaning that anyone who attempted to see collection practices would be in a desperate rat race against a subsequent update. Despite user data being stored in Virginia and Singapore, CFIUS still determined that ByteDance's ownership of TikTok represented a security risk. The question then becomes how user data could be used against a nation's security.

It is also crucial to distinguish ByteDance's practices from Facebook's or Google's, with respect to the international adversarial context. While Facebook may collect and sell data to analytics firms for commercial purposes, ByteDance is largely acting under an acquiescent CCP; a tenuous relationship which could change rapidly. According to James Andrew Lewis with the Center for Strategic and International Studies, China has become a master of espionage, after building the world's largest authoritarian surveillance state against its own citizens, meaning anything that is Chinese owned and connected to the Internet has potential to become a security risk.[51]

This declaration is corroborated yet tempered by Samm Sacks's statement to Senator Sheldon Whitehouse when testifying on Chinese cyber practices, "[u]ltimately the Chinese government can compel companies to turn over their data, but this does not always happen."[52] Sacks, a Senior Fellow at Yale Law School's Paul Tsai

---

[50] Kevin Poulsen, *TikTok Tracked User Data Using Tactic Banned by Google*, WALL ST. J. (Aug. 11, 2020), *available at* https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738 (last visited Nov. 9, 2021).

[51] James Andrew Lewis, *How Scary is TikTok?*, CTR. FOR STRATEGIC & INT'L STUD. (Jul. 14, 2020), *available at* https://www.csis.org/analysis/how-scary-tiktok (last visited Nov. 9, 2021).

[52] Samm Sacks, *Data Security and U.S.-China Tech Entanglement*, LAWFARE (April 2, 2020), *available at* https://www.lawfareblog.com/data-security-and-us-china-tech-entanglement (last visited Nov. 9, 2021).

China Center, argues that Chinese information security issues are too large and ethically ambiguous for individual companies to handle.[53] Data turnover is possible through China's 2017 Cybersecurity Law in Article 28, although experts warn it is incorrect to assume synonymity between Chinese firms and the CCP.[54] It is this murkiness and unpredictability within TikTok's massive collection and popularity that worries lawmakers.

U.S. lawmakers and security experts have started to better understand this context in which TikTok and ByteDance operate. Aside from worries that the CCP could compel ByteDance specifically to furnish collected data, it is undeniable that China as a single entity has increasingly used cyberspace as an advantageous space against the U.S., often targeting personal data. Since 2015, Xi Jinping and Beijing military leaders have increasingly centralized cyber warfare units, while also acknowledging the existence of both military and civilian cyber units.[55] Further, Chinese cyber tactics are particularized, distinguishing between economic espionage, political destabilization, and traditional clandestine intelligence operations.[56]

These aggressive reorganizations and vast networks have yielded immense successes for the CCP. Simply look to the cyberattacks on Pennsylvania State University, the University of Connecticut, and the University of Virginia in 2015 – all institutions hosting research facilities tied to the DoD.[57] In total, the TikTok scenario represents both a changing security landscape and an adversary who knows how to dominate cyberspace.

Unfortunately, even the meager negotiations for increased American ownership have fallen flat as of December 2020. CFIUS could still turn to the DoJ for enforcement of the order as no formal extension of the divestment negotiations has been awarded to ByteDance. Therefore, it seems likely that ByteDance will succeed in the judicial

---

[53] *Id.*
[54] *Id.*
[55] Tremayne Gibson, *2015 a Pivotal Year for China's Cyber Armies,* DIPLOMAT (Dec. 17, 2015), *available at* https://thediplomat.com/2015/12/2015-a-pivotal-year-for-chinas-cyber-armies/ (last visited Nov. 9, 2021).
[56] *Id.*
[57] *Id.*

system but will be forced to divest after CFIUS negotiations conclude amicably or through the DoJ.

As previously mentioned, popular candidates for acquisition include Oracle and Walmart.[58] A preliminary deal stated that Oracle and Walmart would obtain a combined twenty percent stake in TikTok Global, details of which were expected to become public in 2021.[59] Under this deal, four of the five directors on TikTok Global's board would be American, and its headquarters would be located in the U.S.[60] Even further, Oracle would host all U.S. user data on its cloud system and, according to Walmart, the global company would pay $5 billion in new tax dollars to the U.S. Treasury.[61] These efforts are clearly a move to appease concerns of Chinese influence over the company, while allowing ByteDance itself to remain as close as necessary to Beijing. Unfortunately, as of March 2021, negotiations have halted.

However, even this diplomatic option created confusion and concern. At face value it appears that ByteDance could retain eighty percent of TikTok Global before the new entity goes public. Yet Ken Glueck, Oracle Vice President, stated that once TikTok Global shares are distributed Americans will be the majority owners. This ownership transition will occur because shares will be given directly to investors, and nearly forty percent of ByteDance is currently owned by U.S. venture capital firms.[62]

Yet this ownership option did not appease Republican lawmakers nor the White House, and it is unclear what specific

---

[58] Alex Lawson, *Commerce Puts TikTok Restrictions on Hold*, LAW360 (Nov. 12, 2020), *available at* http://plus.lexis.com (last visited Nov. 9, 2021); *see also* John D. McKinnon, *TikTok Sale to Oracle, Walmart is Shelved as Biden Reviews Security*, WALL ST. J. (Feb. 10, 2021), *available at* https://www.wsj.com/articles/tiktok-sale-to-oracle-walmart-is-shelved-as-biden-reviews-security-11612958401 (last visited Nov. 9, 2021).

[59] Andrew Morse & Queenie Wong, *Judge Blocks TikTok Ban as Negotiations with U.S. Continue*, CNET (Dec. 7, 2020), *available at* https://www.cnet.com/news/tiktok-sale-deadline-elapses-as-negotiations-with-us-continue/ (last visited Nov. 9, 2021).

[60] *Id.*

[61] *Id.*

[62] *Id.*

technology would transfer to Oracle. Indeed, ByteDance in the past has demanded ownership of TikTok's algorithm, only allowing Oracle oversight of TikTok's source code. Algorithms in social media apps often run what users are prompted to view and engage with, what advertisements they see, and what content is likely to soar in popularity. For example, if a viewer on YouTube watches several cooking tutorials and subscribes to a home cooking channel, YouTube's algorithm would suggest popular cooking videos to that viewer and promote advertisements based on kitchen items or local grocery stores.

Whereas source codes are programming statements made by a programmer and saved in a file, the algorithm comprises the foundation of how an app will interact with the user.[63] With distinctions between ByteDance and venture firms, a new global entity's ownership, and what technologies will be run by U.S. providers, the tenuous deal is rife with pitfalls.

At the least, the TikTok dilemma exemplifies the need for more concrete legal protections on individual's data if not for their own privacy, for their nation's security. The U.S. is, by many measures, behind in what experts call "the grey zone": aggressive actions not rising to traditional definitions of conflict in cyber-activities. The unbridled popularity of social media platforms represents opportunities for adversaries to gather and use citizens' data against our largely open society. One could imagine social media apps as resource mines in the grey zone which our adversaries can, and have, tapped into.

III. Undeterred Data in a Bordered Globe

Given that data is clearly valuable in a security context, understanding how it is treated in the international political system is crucial to creating more cogent solutions for a more secure globe. In this section I explore the difficulties of data in the international

---

[63] *Source and Object Code*, UNIV. WASH. OFF. RSCH. (2021), *available at* https://www.washington.edu/research/glossary/source-code-and-object-code (last visited Nov. 9, 2021).

sphere, return to discussed regional responses, and argue that the most cogent responses are state-specific and provide potential frameworks which Washington could adopt.

A. DIFFICULTIES

The first consideration is jurisdiction: if data is a product in commerce and a resource in national security, what entity controls or could control it? Unfortunately, as explored in Professors Kenneth Anderson and Jennifer Daskal's "The Un-Territoriality of Data," our current societal framework is simply not optimized for personal data.[64] The piece outlines how data travels in an arbitrary path disregarding property and borders at a pace which surpasses physical materials in international trade.[65] Further, data can be divided up and stored in potentially limitless ways across the globe. Personal data dissemination disregards our traditional framework of sovereignty and borders, so already one can see that crafting an international solution on data regulation is difficult.

Perhaps this explains why some experts in the field, such as Anderson and Daskal, warn against primary state access of data in the international system. Users lack control over what path data takes and as mentioned, the path is often arbitrary. This was stated in a case involving Microsoft in which experts warned that outcomes would be largely arbitrary if government access to data was location dependent.[66] Further, data divisibility, a common practice of dividing data across many servers, means that multistate storage has constantly been used to increase data's efficiency in an increasingly interconnected globe.[67]

A common solution some governments have taken is analogizing cross border data access to extraterritorial killings. The upshot is that the target's location controls, regardless of the operator of the weapon, such as in *Hernandez v. United States* or *United States v. Gorshkov*.[68] But the analogy is tenuous at best, as with data there is

---

[64] Jennifer C. Daskal, *The Un-Territoriality of Data*, 125 YALE L. REV. 326 (2015).
[65] *Id.*
[66] *Id.* at 367.
[67] *Id.* at 368.
[68] Hernandez v. United States, 757 F.3d 249, 255 (5th Cir. 2014) (involving a scenario in which a border agent in Texas shot and killed a fifteen-year-old

no tangible or even noticeable exchange between states. Even more, the user's ability to access the data is unchanged, whether the user desires them to do so or not, the user would not likely notice if a government or business had access. It is this point which Professor Daskal emphasizes that where the data is being accessed and transported to controls, not the location of its storage.[69] Overall, data represents a stubborn problem for individual governments and, by extension, bilateral relationships.

B. INTERNATIONAL ATTEMPTS

An international consideration of data quickly becomes complex when state sovereignty, jurisdiction, data ownership, and the consent of the private individual are considered.[70] While some may scoff at how respected privacy might be on a global scale, privacy is enshrined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which forms conversations leading to tangible reforms, such as the Organization for Economic Cooperation on Development's view on trans-border data flows.[71] However, it appears that some states and intergovernmental unions are taking the initiative. The current trend for developing international data privacy norms acknowledges a form of individual privacy rights from a humanitarian perspective, with unions such as the E.U. and international organizations increasingly stipulating informational privacy standards.[72]

Mexican), *rev'd en banc, rev'd per curium*, 785 F.3d 117 (5th Cir. 2014), *petition for cert. filed*, No. 15-118 (U.S. July 27, 2015); Rodriguez v. Swartz, No. 4:14-CV-02251 (D. Ariz. Jul. 9, 2015) (involving a scenario in which a border agent in Arizona shot and killed a sixteen-year-old Mexican), *see also* United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).

[69] Reinsch, *supra* note 47, at 373.

[70] *See* Kate Westmoreland, *The Global Corporate Citizen: Responding to International Law Enforcement Requests for Online User Data*, HARV. J. L. & TECH. JOLT DIG. (2015), *available at* https://perma.cc/MD44-SKRV (last visited Nov. 9, 2021).

[71] Javier Lopez Gonzalez, *Hitchhiker's Guide to Cross-Border Data Flows*, ORG. FOR ECON. CO-OPERATION & DEV. (June 3, 2019), *available at* https://www.oecd.org/trade/hitchhikers-guide-cross-border-data-flows/ (last visited Nov. 9, 2021).

[72] *See* Theodore J. Kobus et al., *2015 International Compendium of Data Privacy Laws* iv, BAKERHOSTETLER (2015), *available at* https://docplayer.net/1572007-

While this new legal norm slowly encourages even the most skeptical members of the international community to accept data privacy, unfortunately, it allows states to adopt exceptions in the name of national commercial competition. Further, the focus is on the rights of the individual against imposing corporations without recognizing how some bad actors actively target individual's data. It is therefore useful to observe how individual states have decided to address individual data protection, efforts which could act as a framework for hypothetical global agreements for Washington to build from.

i. Data Localization

The most user-protective system for handling data on an international scale is data localization. This method requires citizens' data to be collected, processed, and stored within those citizens' country before travelling across borders. The data cannot transcend borders before meeting local privacy standards and obtaining the individual's consent; which is often in the terms of agreement.[73]

The EU's GDPR is the cornerstone example of cogent data localization. Adopted in 2016, the EU desired to standardize data security laws across the union while also requiring individual consent, the anonymization of collected data, data breach notifications, and the regulation of data transfers across borders.[74] The GDPR applies to any company that even markets its goods or services to EU citizens, creating a global impact. Companies face intense penalties for non-compliance, issued by Supervisory Authorities who can also promulgate warnings, perform audits, order

---

2015-international-compendium-of-data-privacy-laws.html (last visited Nov. 9, 2021).

[73] Courtney Bowman, Comment, *Data Localization: An Emerging Global Trend*, JURIST (Jan. 6, 2017), *available at* https://www.jurist.org/commentary/2017/01/courtney-bowman-data-localization/ (last visited Nov. 9, 2021).

[74] Juliana De Groot, *What is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019*, DIG. GUARDIAN (Sept. 30, 2020), *available at* https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection (last visited Nov. 9, 2021).

data to be erased, or even block companies from transferring data across borders.[75] Indeed, the GDPR represents an extensive protectionist move which has engendered a variety of protection laws in other countries, some less stringent and others even more demanding.

ii. Lesser Protections Creating Discord

Some countries such as the U.S. offer fewer protectionist methods in the aim of expedited data transfers, often with commercial advantages in mind. The U.S. has no single federal law on user data privacy, and most develop through trade deals, such as the EU-US Privacy Shield of 2016.[76] Even this agreement has faced a litany of legal challenges within the EU from parties who still hold U.S. standards to be inadequate.

As these commercial conflicts begin to arise amongst security risks, individual U.S. states have begun to search for a solution which balances its economic goals with user privacy. These can range from comprehensively strong policies, such as California's Consumer Privacy Act of 2018 ("CCPA") to more niche bills such as Illinois' Geolocation Privacy Protection Act ("HB2785") which defines geolocation and requires private entities obtain user consent to collect it.[77] However, as of January 2021, HB2785 is *sine die*; like some thirty states, the Illinois legislature has yet to completely adopt its measures.[78]

Complicating this already fragmented response, some U.S. states have chosen to push forward breach notification laws, forcing

---

[75] *Id.*

[76] Commission Implementing Decision 2016/1250 of July 12, 2016, of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207/1).

[77] *2020 Consumer Data Privacy Legislation*, NAT'L CONF. OF ST. LEGISLATURES (Jan. 17, 2021), *available at* https://www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx (last visited Nov. 9, 2021).

[78] H.B. 2785, 101st Gen. Assembly, Reg. Sess. (Ill. 2021).

compromised entities to notify consumers of cybersecurity breaches. Such laws are often focused on the financial or healthcare sectors.[79]

In addition to the vast variety of state frameworks, the U.S. Federal Trade Commission has jurisdiction over several commercial entities to protect individuals against unfair privacy or data security practices.[80] While this new legal norm slowly encourages even the most skeptical members of the international community to accept data privacy, unfortunately, it allows states to adopt exceptions in the name of national commercial competition. Further, the focus is on the rights of the individual against imposing corporations without recognizing how some bad actors actively target individual's data. It is therefore useful to observe how individual states have decided to address individual data protection, efforts which could act as a framework for hypothetical global agreements for Washington to build from.

iii. Authoritarian Protections

As previously discussed, the CCP has created a standard of individual data protection which simultaneously protects Chinese citizens from foreign companies harvesting their data. Chinese laws also bar any potential for state adversaries to do the same while also surveilling its citizenry to dystopian levels.

Although the Great Firewall has existed since 2000, and even faced occasional backlash with every passing year the CCP hands down another restriction on what is allowed onto Chinese citizens' devices.[81] This serves two purposes: not only blocking out information but creating a digital echo chamber for Party propaganda. Such was the case in 2013 with Document No. 9, a Party document outlining

---

[79] Cynthia Brumfield, *12 New State Privacy and Security Laws Explained: Is Your Business* Ready, CSO (Dec. 28, 2020), *available at* https://www.csoonline.com/article/3429608/11-new-state-privacy-and-security-laws-explained-is-your-business-ready.html (last visited Nov. 9, 2021).

[80] *Data Protection Laws in the United States*, DLA PIPER (Jan. 28, 2021), *available at* https://www.dlapiperdataprotection.com/index.html?t=law&c=US (last visited Nov. 9, 2021).

[81] Yaqui Qang, *In China, the "Great Firewall" Is Changing a Generation*, HUM. RTS. WATCH (Sept. 1, 2020), https://www.hrw.org/news/2020/09/01/china-great-firewall-changing-generation (last visited Nov. 9, 2021).

"seven perils" which were to be cracked down on, namely free press, uncontrolled education, and the Internet.[82] Indeed, every possible information outlet is censored in some form. Politico researcher Yaqui Wang notes that with every generation the Great Firewall yields more success in the eyes of the CCP.[83] Each passing generation has seen fewer and fewer images, texts, or platforms beyond what the Party considers acceptable.[84]

Returning to personal data specifically, in November 2020, the Personal Information Protection Law ("PIPL") was passed, a universal law governing any entities operating in China who process personal data.[85] In reading the new layer of protection, some similarities between PIPL and the GDPR arise, such as how foreign companies must pass a security assessment even if the data is stored outside of China's borders.[86] Layering this new law on top of discussed surveillance and censorship practices, in addition to China's knack for intellectual property theft, the country has become a major force in cyberspace; often to the detriment of the U.S.[87] This level of influence does not just impact victims, however.

Startlingly, as the superpower continues to rise it has attempted to make its norms more acceptable. It is a desirable thought that any authoritarian model of individual data protection would be inapplicable to the U.S. and impossible on a global scale. Here, it would require rejection of political and legal doctrines intrinsic in American society. On an international level, it would require a unipolar system lead by a hegemonic China with the resources and political will to complete global censorship in the

---

[82] *Id.*
[83] *Id.*
[84] *See* Wang, *supra* note 86.
[85] Thomas Zhang, *China's Personal Information Protection Law: Compliance Considerations from an IT Perspective*, CHINA-BRIEFING, (Dec. 11, 2020), https://www.china-briefing.com/news/data-privacy-china-personal-information-protection-law-it-compliance-considerations/#:~:text=China%20too%20released%20its%20draft,law%20on%20protecting%20personal%20information (last visited Nov. 9, 2021).
[86] *Id.*
[87] *Chinese Malicious Cyber Activity*, CYBERSECURITY & INFRASTRUCTURE AGENCY (n.d.), https://us-cert.cisa.gov/china (last visited Nov. 9, 2021).

name of protection. The idea seems to be the stuff of dystopian nightmares.

However, several authors with the Center for Security and Emerging Technology write that in the field of artificial intelligence ("AI") this very concept is playing out.[88] Russia and China have become major exporters of surveillance and censorship technology to hundreds of countries; and with those technologies dissent suppression and public opinion quashing are exported.[89] By giving these actors room to work in this area, the U.S. has de facto accepted the potential spread of authoritarian practices and by so many measures the situation in cyberspace is dire.

IV. Conclusion: An Unprepared Nation, an Insecure Battle, with at-risk Individuals

Returning to the first acknowledgment in this Note, the stage for interacting with other states is becoming increasingly digital. Data of all kinds is used by companies and state governments alike with revolutionizing tactics; be it commercial, diplomatic, or adversarial. Due to the United States' reliance on traditional intelligence and conflict measures, state led initiatives, and adherence to private industry responses, the country is especially unprepared in cyberspace's "gray zone": an area of conflict below traditional measures but certainly antagonistic.[90]

The use of the gray zone is not unheard of or even new in many contexts, such as geopolitics. Simply look to China's activities in the South China Sea: redrawing borders, sailing fleets, and crafting artificial islands in contested areas – all certainly not

---

[88] *See generally*, ANDREW IMBRIE ET AL., CENTER FOR SECURITY AND EMERGING TECHNOLOGY, AGILE ALLIANCES (2020).

[89] *Authoritarians are Exporting Surveillance Tech, And With it Their Vision for the Internet*, COUNCIL ON FOREIGN REL. (Dec. 5, 2019), *available at* https://www.cfr.org/blog/authoritarians-are-exporting-surveillance-tech-and-it-their-vision-internet (last visited Nov. 9, 2021).

[90] *See* Lindsey R. Sheppard & Matthew Conklin, *Warning for the Gray Zone*, CTR. FOR STRATEGIC & INT'L STUD. (Aug. 13, 2019), *available at* https://www.csis.org/analysis/warning-gray-zone (last visited Nov. 9, 2021).

peaceful but not rising to the level of traditional conflict.[91] Or, perhaps more on point here, consider Russia's cyberactivity in European elections and Central European power grids, activities which undermine the very institutions democracies rely on, yet were not recognized as a threat until it was too late.[92] One can see that this gray zone is expanding in potential, and with an expanding reliance and use of cyberspace, individual data is being used in that gray zone.

The implications of private data in the national security context within this gray zone are concrete, the Senate Select Committee on Intelligence commissioned an investigation after the 2016 U.S. Presidential Election into how third parties accessed user's data collected by social media platforms.[93] Private data could be hacked, sold to third parties anywhere in the world, or acknowledged by an adversary's intelligence community and exploited; all likely without the individual knowing of their breach and potential manipulation.[94] Private data could be hacked, sold to third parties anywhere in the world, or acknowledged by an adversary's intelligence community and exploited; all likely without the individual knowing of their breach and potential manipulation.[95] This is not a foreign issue either; although the successes of Chinese tech companies like ByteDance or Huawei's 5g network expansions commonly make headlines, even U.S. headquartered companies like Equifax remain a potential Achilles' heel.[96]

Nonetheless, China's strides in AI and its insular technology policies have awoken lawmakers for good reasons. Beyond the real

---

[91] LYLE J. MORRIS ET AL., GAINING COMPETITIVE ADVANTAGE IN THE GRAY ZONE xiii-37 (Rand Corp. 2019).
[92] *See id.* at 91.
[93] Carrie Cordero, *The National Security Imperative of Protecting User Data*, CTR. FOR A NEW AM. SEC. (Apr. 24, 2019), *available at* https://www.cnas.org/publications/commentary/the-national-security-imperative-of-protecting-user-data (last visited Nov. 9, 2021).
[94] *See id.*
[95] *Id.*
[96] Robert D. Williams, *To enhance data security, federal privacy legislation is a start*, BROOKINGS INST. (Dec. 1, 2020), *available at* https://www.brookings.edu/techstream/to-enhance-data-security-federal-privacy-legislation-is-just-a-start/ (last visited Nov. 9, 2021).

possibility of Beijing commandeering magnates such as ByteDance and all its collected data, its advancement in AI technologies is astounding with potential civilian and military applications.[97] AI is reliant on data collected in an algorithmic fashion but is limitless in application once well-developed. Thus, controlling how much data that algorithm receives is crucial in preventing that AI's development and adversarial uses. Simply put, a federal law protecting individual data here would limit the number of building blocks available to a Chinese AI program.

Professor Susan Aaronson confirms the trends and practices just discussed, arguing that the U.S. needs a comprehensive approach after years of negligence.[98] Alluding to breakthroughs in the gray zone, Aaronson points to the 2013 hack of Target, J.P. Morgan, and the U.S. Office of Personnel Management as the event when Washington was put on notice that data was an at-risk resource with an adversarial China.[99] With the explosion of social media since, Aaronson suggests that the U.S.' slow response is largely due to the fact that most social media and internet titans are American companies.[100]

The situation has changed, however, after years of consumer and capital build-up in an insulated domestic market, Chinese companies have the capacity to outpace U.S. ones, something less palatable to U.S. lawmakers than unregulated American titans. Aaronson concludes with an urge for comprehensive data protection reforms across the board, which would protect individuals, hold every data collecting entity accountable, and streamline data transfers with our allies.[101]

Writing for *Lawfare* from the Tsai China Center at Yale Law, Robert D. Williams affirms the need for an overhaul of how the U.S. allows private companies to treat individual data – both in the

---

[97] *Id.*

[98] Susan Ariel Aaronson, *Why Personal Data is a National Security Issue*, BARRON'S (Aug. 12, 2020), *available at* https://www.barrons.com/articles/why-personal-data-is-a-national-security-issue-51597244422 (last visited Nov. 9, 2021).

[99] *Id.*

[100] *Id.*

[101] *Id.*

interests of the citizen and the security interests of the nation.[102] Williams quarrels with Samm Sacks's and Jennifer Daskal's call for developing set standards which address privacy and protection rather than "trying to clip the wings of rising entrants."[103] In 2019, Williams disagreed with Sacks's and Daskal's critique of Washington's reliance on CFIUS and case-by-case review of every foreign Internet entity, describing CFIUS as a "scalpel" rather than a defensive "sledgehammer."[104] Nonetheless, experts such as Aaronson, Sacks, Daskal, and now even Williams in 2020 have recognized the need for Washington to take the initiative and put down the scalpel.

Indeed, while it is unfortunate that it took a foreign tech company to revitalize the discussion of federal protections, adopting cohesive protections would tackle several key areas of concern: national security, international cohesion, and personal privacy. Clearly new legislation would aim at protecting private data through a national security lens, but a national standard would reduce compliance costs for existing U.S. companies, increase confidence in our allies such as the EU, and build protections against potential foreign adversaries, such as ByteDance to active adversaries like North Korea.[105]

Further, as Robert Williams notes, by adopting legislative policy based on standards and principles rather than executive orders carving out specific countries, we are protected from critiques of hypocrisy.[106] Again, consider how many American statesmen and thinktanks critique the CCP's practices of banning specific websites and platforms – even this piece acknowledged Beijing's sprawling censorship. Without proper legislation or divestment to American

---

[102] Robert D. Williams, *Reflections on TikTok and Data Privacy as National Security*, LAWFARE (Nov. 19, 2019), *available at* https://www.lawfareblog.com/reflections-tiktok-and-data-privacy-national-security (last visited Nov. 9, 2021).

[103] *Id.*

[104] *Id.*

[105] Robert D. Williams, *To enhance data security, federal privacy legislation is a start*, BROOKINGS INST. (Dec. 1, 2020), *available at* https://www.brookings.edu/techstream/to-enhance-data-security-federal-privacy-legislation-is-just-a-start/ (last visited Nov. 9, 2021).

[106] *Id.*

firms the U.S. would, through executive orders, essentially be doing the same while cheering for market capitalism.[107] By acting through legislative policy, Washington could bolster data security while sending a signal of our adherence to liberal norms to our liberal democratic allies.

A. FORWARD

At the beginning, this Note touched on the humaneness of privacy. To many legal scholars privacy is crucial to autonomy, self-protection, and by extension, democratic society.[108] Personal privacy is not only enshrined in the U.S. Constitution but is found, perhaps even more concretely, in the United Nations Declaration of Human Rights of 1948 and the International Covenant on Civil and Political Rights of 1966.[109] Indeed, privacy is a human right crucial in modern society and is deserving of protection in that measure alone.

Yet the digital age presents new spaces for conflict with new resources, as explored here, cyberspace and personal data. Even more, global ecommerce draws upon personal data as a new means of effective yet highly intrusive marketing. Therefore, states have been compelled to act and protect private data either from a place of concern for individual rights, state security, or perhaps a marriage of both. This is exemplified through the European Union's GDPR, which upholds individual privacy against intrusive companies and adversarial states, or through China's Personal Information Protection Law – alongside a variety of censorship laws which aim to maintain the CCP's security.

The U.S. is falling behind on a critical issue which impacts individual privacy and its own national security. Given that widespread censorship would be unpalatable in the minds of American lawmakers and citizens, Washington should strive for a personal data privacy law modeled after the European Union's GDPR which would hopefully compel private companies to be more

---

[107] De Groot, *supra* note 82.

[108] Olmstead v. United States, 277 U.S. 438, 471-85 (1928) (Brandeis, J., dissenting).

[109] *What is Privacy*, PRIVACY INT'L (Oct. 23, 2017), *available at* https://privacyinternational.org/explainer/56/what-privacy (last visited Nov. 9, 2021).

open about their collection processes while also demanding that those companies store collected data within the U.S. Further, this would hopefully spark litigation against bad actors and the misuse of personal data.

What D.C. should do does not end there, however, as the existence of cyber espionage and massive entities such as ByteDance present a serious and continuing issue. Washington needs to reckon with the fact that cyberspace has become the new medium in which geopolitical struggles develop. Our adversaries certainly have: look to Russia's extensive use of data and cyberspace as a means of spreading disinformation and rattling faith in electoral processes with a regularity some experts consider replicative of wartime strategy.[110] Or look to China's variety of actions in cyberspace, from censorship to IP theft and data protection to espionage.[111] Indeed, the U.S. has been slow to accept that our adversaries use of cyberspace has reached aggressive levels, and needs a more centralized and assertive approach rather than the existing network of passive entities.[112]

---

[110] Garret M. Graff, *A Guide to Russia's High Tech Toolbox for Subverting Democracy,* WIRED (Aug. 13, 2017), *available at* https://www.wired.com/story/a-guide-to-russias-high-tech-tool-box-for-subverting-us-democracy/ (last visited Nov. 9, 2021).

[111] Lyu Jinghua, *What Are China's Cyber Capabilities and Intentions,* CARNEGIE ENDOWMENT FOR INT'L PEACE, *available at* https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734 (last visited Nov. 9, 2021).

[112] Adrien Chorn and Monica Michiko Sato, *Maritime Grey Zone Tactics*, CTR FOR STRATEGIC AND INT'L STUD., *available at* https://www.csis.org/maritime-gray-zone-tactics-argument-reviewing-1951-us-philippines-mutual-defense-treaty (last visited Nov. 9, 2021).