Toward a Comprehensive Understanding of Artificial Intelligence in International Affairs

Dear readers:
This is very much a work in progress, and some of the sections, especially in Part III, I consider to be rather inchoate. I have left various notes to myself throughout the draft in the hopes that you will at least understand what my intentions are even if I have not yet articulated them adequately. I appreciate your feedback and thank you for reading my paper. If you have additional written comments, please send them to me at jwwoo2 "at" gmail.com.

Introduction

This essay will explore the likely implications and stakes of the global competition in artificial intelligence (AI) and machine learning (ML), and how strong data privacy and algorithmic fairness, accountability, and transparency (FAT) rules could be an advantage rather than a hindrance in that competition. It will examine the likely influence of AI in international affairs using the framework laid out by George Weiss, the longtime Georgetown scholar and pioneer of the field of science, technology, and international affairs (STIA). Much of the recent discussions of this issue have principally focused two narrow topics: economic competition between the U.S. and China to gain an advantage with this technology and the impact of AI on military power. This essay will seek to be more comprehensive, applying Professor Weiss' framework to understand the broader implications of AI in international affairs. There is a general sense that AI is an important technology, but less examination of why that is the case. This essay gives special attention to the importance of data to most ML techniques and notes the central role of access to data and privacy in some contemporary cross-border trade issues. Extraterritorial regulation by the U.S. and EU have sought to use domestic legislation to promote their own visions of data access, in line with theories of global public goods in international affairs. I posit that by strengthening certain privacy FAT rules, the U.S. and her allies may be able to promote privacy as a global public goods and create a privacy race to the top.

Judging by the actions of U.S. policy makers, two fears dominate the discussion of AI's role in international affairs, both of them relating to American competition with other States, particularly China. The first is that AI and related technologies will deliver a major economic boon to the firms that are able to develop and implement them, and first at scale. The country with the greatest number of AI power houses will benefit from a "second machine age" that brings prosperity and the national security that comes with economic strength. The second fear is that AI offers benefits of speed and efficiency to militaries and national security agencies, so if the American defense industry fails to adopt this technology it will lose its asymmetrical advantage over other states.

These concerns are real and pressing, however they are not the entire picture. A major goal of this essay is to use Professor Weiss' framework to understand and elevate the overlooked aspects of AI's influence on international affairs. STIA is a sub-discipline of international relations that seeks to explain the impact of technology on the international political order and the relationship between States. Professor Weiss posits that science and technology affect international affairs in four categories: 1) by "changing the processes by which the international system operates," 2) by

"changing the architecture of the international system," 3) by "creating new issue areas, new constraints and trade-offs in the operational environment of foreign policy," and 4) by "providing a source of changed perceptions, of information and transparency for the operation of the international system."[1] The impact of nuclear weapons and telecommunications technologies have been important topics for STIA in the past. With AI poised to become the next major transformative technology, its impacts on each of these categories will be similarly profound. However, much of the writing on this topic has addressed the military implications of AI or trade practices of the U.S and China.[2] Take, for instance, discussions about reforming the Committee on Foreign Investment in the United States (CFIUS), or the need for a U.S. national strategy on AI.[3] Such work addresses Professor Weiss' third category, treating AI as a new substantive policy area in international affairs. This paper's goal is to address all facets of AI's influence on international affairs, including the other three categories.

This paper argues that because data is so important to current machine learning techniques, a nation's laws regarding data use could impact not only its own AI economy but the global AI ecosystem as well. It will focus on ML, the sub-field of AI that has been responsible for most of its recent advances. The fact that ML relies on large amounts of data from which to learn will have important impacts on how countries deploy this technology. The U.S. and EU have already experimented with unilaterally influencing global rules and norms about data through the CLOUD act and the General Data Protection Regulation (GDPR) respectively. Recent scholarship on global public goods has examined how unilateral action by countries can promote public goods such as security or the rule of law without the need for consent that is inherent in traditional international law frameworks.[4]

This essay will also use a global public goods analysis to examine how to promote open and democratic uses of AI in the international arena. I explore how rules and norms favoring privacy, and FAT algorithms can tip the playing field away from authoritarian uses of AI where they might otherwise have an advantage because of superior access to data. Instead of engaging in a race to the bottom with Chinese AI companies to erode privacy protections, requirements for transparency and fairness could force Chinese companies to play by the rules of western countries, rather than the other way around. This approach is likely to be more effective than relying on only CFIUS reform and/or export restrictions.[5]

I will proceed in three Parts. Part I will establish the stakes for AI in international affairs based on Professor Weiss' comprehensive framework. Part II will review the literature on global public

[1] Charles Weiss, *Science, technology and international relations*, 27 TECH. IN SOC. 295 (2005).
[2] Michael C. Horowitz, *The Algorithms of August*, FOREIGN POL'Y (Fall 2018).
[3] Ben Scott, Stefan Heumann, & Philippe Lorenz, *Artificial Intelligence and Foreign Policy*, STIFTUNG NEUE VERANTWORTUNG (2018); William A. Carter, Emma Kinnucan, & Josh Elliot, *A National Machine Intelligence Strategy for the United States*, CENTER FOR STRATEGIC & INT'L STUDIES (2018); Michael C. Horowitz, Gregory C. Allen, Edoardo Saravalle, Anthony Cho, Kara Frederick, & Paul Scharre, *Artificial Intelligence and International Security*, CENTER FOR NEW AM. SECURITY (2018).
[4] Nico Krisch, *The Decay of Consent: International Law in an Age of Global Public Goods*, 108 AM. J. INT'L L. 1 (2014).
[5] Empowered by the 2019 National Defense Authorization Act, the Trump administration recently posted an advanced notice of proposed rulemaking for export restrictions on "emerging technologies" that includes AI and ML. 15 CFR 744 (2018). See also Cade Metz, *Curbs on A.I. Exports? Silicon Valley Fears Losing Its Edge*, NY Times Jan. 1, 2019. https://www.nytimes.com/2019/01/01/technology/artificial-intelligence-export-restrictions.html

goods and recent actions by the U.S. and EU to unilaterally influence global data norms. Part III will examine how domestic actions or partnerships between the U.S. and her allies might use strong privacy rules to create a race to the top that promotes AI that is fair, accountable, and transparent.

Part I

[Insert basic background on ML and AI that everyone here already knows so I'm not going to bother with now. Key point is that it requires lots of data and lots of compute.]

A. A Framework for Understanding Technology's Influence on International Affairs

Professor Weiss proposes a four part framework for science and technology's impact on international affairs, and AI is likely to touch on each category. Weiss is a PhD chemist and the first Science and Technology advisor to the World Bank. He later joined the faculty at the Georgetown School of Foreign Service and directed its STIA program. During that time he proposed a framework to understand how science and technology impact international affairs, and vice versa. He writes that technology influences international affairs in four key areas: its architecture, its information flows, its substance, and its processes. This section will explore how AI's is likely to fit into each category. My hope is that by approaching this topic systematically and categorically, I can identify gaps or blind spots in the current debate.

1. Changing the processes by which the international system operates

Professor Weiss describes the "operational processes of the international system" as including actions "carried out predominantly by governments–diplomacy, war, administration, policy formation, crisis management, and the gathering of intelligence," and "those carried out predominantly by the private sector—commerce, trade, economic competition, finance, communications, and most directly from the point of view of science and technology, the management and financing of research and innovation."[6] He notes that advances in weaponry and network technology now require policy makers to act at "Internet speed."[7] He also says that technology changes the relationships between actors, such as between aggressors and defenders in military conflicts, regulators and the regulated, buyers and sellers, etc.[8] Technology also blurs distinctions between previously important categories, such as between combatants and non-combatants in cyber conflict.[9]

AI has already begun to make its way into both public and private sector processes that have international ramifications. China has begun to implement a program that use AI to game out the strategic consequences of different policy decisions.[10] The AI will make use of a vast array of data inputs, ranging from "cocktail-party gossip to images taken from spy satellites."[11] A human

[6] Weiss at 299-300.
[7] Weiss at 300.
[8] *Id.*
[9] *Id.*
[10] https://www.scmp.com/news/china/society/article/2157223/artificial-intelligence-immune-fear-or-favour-helping-make-chinas.
[11] *Id.*

diplomat will be in-the-loop and responsible for any ultimate decisions, but proponents tout the fact that "[i]t would not even consider the moral factors that conflict with strategic goals."[12] The use of AI in strategic planning and decision making goes beyond simple efficiency gains and speed of decisions. When an AI system beat the world champion of the board game Go, analysts noted that it used some strategies that had never been contemplated in the game's 2500 year history.[13] An AI may be able to do something similar in planning an armed conflict or strategizing trade negotiations.[14] A country might be able to use an AI to deduce information being hidden by a counter-party in other strategic negotiations, like a game of poker with much higher stakes.

AI has already been put to limited military use, and this use will likely increase. Project Maven famously, and controversially, aims to help the U.S. Department of Defense (DoD) process and analyze large quantities of visual data using computer vision.[15] The U.S. military has also expressed an openness to lethal autonomous weapons (LAWs) that can attack and kill a person without the explicit command of a human operator.[16] The development of such a weapon has not been confirmed and is largely speculative at this point. However, South Korea has deployed the SGR-A1, a stationary gun turret that can autonomously identify human targets, along the demilitarized zone between South and North Korea.[17] It is believed SGR-A1 employs a human-in-the-loop (HITL) system, where a human operator must affirmatively act to fire upon a target.[18] AI systems have also been tested to control fighter jets in simulation and have prevailed against human pilots under those conditions.[19] For the moment, the U.S. military maintains policy guidance that a human must make any decision to employ lethal force,[20] and has limited facial recognition on weapon systems to targeting assistance.[21] The use of LAW systems is naturally controversial; opponents argue that LAWs could reduce the barriers to entry for war by replacing human soldiers with robotic ones, among other worries.[22] The military could make many uses of AI that are more mundane than killer robots, yet nonetheless offer significant benefit. For instance, the Air Force is experimenting with using AI to monitor aircraft to improve maintenance schedules and predict equipment failures.[23] AI could also create efficiency in military organizational processes such as program management, evaluation, and hiring that are similar to uses in the private sector.

The military is far from the only branch of government that could benefit from AI of course; the State department operates the day to day organs of American diplomacy and could potentially employ AI in several ways. State engages in a great deal of large scale yet repetitive information

---

[12] *Id.*
[13] Cite
[14] https://www.brookings.edu/research/the-impact-of-artificial-intelligence-on-international-trade/
[15] https://dod.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/.
[16] https://www.popularmechanics.com/military/research/a23133118/us-ai-robots-warfare/.
[17] https://www.lawfareblog.com/foreign-policy-essay-south-korean-sentry%E2%80%94-killer-robot-prevent-war.
[18] https://www.lawfareblog.com/foreign-policy-essay-south-korean-sentry%E2%80%94-killer-robot-prevent-war
[19] https://www.omicsonline.org/open-access/genetic-fuzzy-based-artificial-intelligence-for-unmanned-combat-aerialvehicle-control-in-simulated-air-combat-missions-2167-0374-1000144.pdf.
[20] https://www.hsdl.org/?abstract&did=726163.
[21] https://www.bbc.com/news/technology-47524768.
[22] https://www.stopkillerrobots.org/learn/.
[23] DoD Strategy

processing tasks that could be supplemented by AI. The screening of passport and visa applications for errors and other omissions is currently done manually by large numbers of federal employees.[24] Diplomats in the U.S. and elsewhere must also process a great deal of information in order to formulate policy. Machine learning could help them discern patterns or otherwise process large amounts of data. For instance, the State Department oversees several billions of dollars' worth of foreign aid and programs, and monitoring these programs for efficacy and fraud detection is a significant undertaking. AI could also give insights of where money could be spent most effectively; essentially a form of enhanced evidence-based policy making. It could also be employed to find patterns of international money laundering, strengthen economic sanctions enforcement, or otherwise improve the "economic and financial tools of statecraft."[25] On the other hand, bad actors may be able to use it to evade detection and skirt international law.[26] This problem could be exacerbated if such AI tools become easily accessible. Currently, many AI tools require some combination of technical expertise, large datasets, and high compute to develop and implement.[27] If they can be packaged to be used off the shelf, then terrorist groups and criminal organizations could pose additional challenges for law enforcement.

The intelligence community (IC) can and likely already does use AI in a number of ways for both intelligence gathering and counter-intelligence. Researchers at the Harvard Belfer Center note that the IC currently collects more data than it can reasonably analyze and use, but that ML techniques could help draw useful conclusions, finding the proverbial needle in the haystack.[28] The ability to use AI to create fake but convincing digital photos and videos could exacerbate foreign propaganda and "active measure" campaigns like the one that struck the 2016 U.S. presidential election. AI has also created a number of powerful new surveillance techniques that can make it much easier for spies or terrorists to operate undetected. Professor Ashley Deeks describes how widespread facial recognition in China could make it quite difficult for human intelligence assets to operate in the country.[29] And researchers are currently working on even more advanced techniques, such as using AI to track human movement through walls based on WiFi signals.[30] Many in both the private and public sector have also begun to implement ML in cybersecurity, although it is still unclear whether this trend will give a greater advantage to cyber offense or defense.

Private sector uses of AI may have duel civilian and military uses or otherwise impact international affairs. Already, much of the trading on the stock market is conducted by high-frequency trading algorithms with no HITL.[31] The use of such algorithms has contributed to flash crashes and other volatility in the stock market in the U.S. and elsewhere.[32] Similar

[24] Review by a federal employee is required by law. Cite
[25] CNAS, AI and International Security, at 7-9.
[26] *Id.*
[27] This is not true of all AI tools however. The Deepfake algorithm is a notable example of a potentially malicious tool that has become democratized.
[28] Belfer Center, AI and National Security
[29] https://www.lawfareblog.com/chinas-total-information-awareness-second-order-challenges.
[30] https://motherboard.vice.com/en_us/article/a3aaqp/mit-device-uses-wifi-to-see-through-walls-and-track-your-movements
[31] Frank Pasquale, Black Box Society
[32] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/289016/11-1226-dr7-crashes-and-high-frequency-trading.pdf

problems may arise as the financial sector implements AI in other areas of banking and finance. AI has also shown promise in solving traveling salesman problems, which could lead to large gains in logistical efficiency in a range of applications from international trade and shipping to military logistics.[33] Some civil society groups have experimented with using AI to predict the outbreak of famine, disease, or genocide in order to prevent or mitigate the impact of humanitarian crises.[34] In such cases, being able to move persons and resources faster, more efficiently, and in some cases preemptively could give the actors employing the AI system a greater ability to influence world events. Just as widespread deployment of rail networks changed transportation logistics and contributed to the industrialization of warfare,[35] AI's ability to improve logistics could have significant and unpredictable influences on geopolitics.

Though AI presents significant potential to improve government and private sector processes in the realm of international affairs, there has been relatively little discussion of how to actually implement such systems from a technical or policy perspective. DoD's AI strategy document references guidelines from 2012 on the use of autonomous and semi-autonomous weapons, as well as research investments in reliability, safety, security, and explainability.[36] It's Joint Artificial Intelligence Center (JAIC) is meant to coordinate these efforts and develop policy.[37] While the State Department does not appear to have any publicly available policy on AI, President Trump's "Executive Order on Maintaining American Leadership in Artificial Intelligence"[38] calls for greater investment in research, education, and job training to promote AI, and to increase access to data held by federal agencies, but speaks only briefly to agencies that would deploy AI themselves.[39] The bipartisan "AI in Government Act" would form an emerging technology policy lab within the federal government to provide technical and policy expertise.[40] This lab would help the government develop law and policy for AI as well as help it to procure and implement AI in its own processes.[41]

2. Changing the architecture of the international system

Professor Weiss defines the architecture of the international system as "(1) its structure, (2) its key organizing concepts, and (3) the relationship among its constituent states and other actors."[42] An example of a change in the international system's structure could be the shift from bipolarity

[33] Stanley Brucal & Elmer P. Dadios, Comparative Analysis of Solving Traveling Salesman Problem using Artificial Intelligence Algorithms; http://www.wseas.us/e-library/conferences/2012/CambridgeUK/AIKED/AIKED-21.pdf.
[34] Famine: https://www.vox.com/policy-and-politics/2018/9/29/17915222/famine-world-bank-south-sudan-yemen-food-crisis-conflict; disease: https://phys.org/news/2018-02-artificial-intelligence-infectious-diseases.html; genocide: https://motherboard.vice.com/en_us/article/539ngd/this-algorithm-could-show-when-the-next-genocide-is-about-to-happen.
[35] Francis J. Gavin, "Crisis Instability and Preemption: The 1914 Railroad Analogy," in Understanding Cyber Conflict: 14 Analogies, ed. George Perkovich and Ariel E. Levite (Washington, DC: Georgetown University Press, 2017), 111-122
[36] Summary of DoD AI Strategy at 15.
[37] *Id.* at 4
[38] https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/
[39] *Id.* § 3.
[40] https://www.congress.gov/bill/115th-congress/senate-bill/3502/text?format=txt.
[41] *Id.*
[42] Weiss at 301.

to monopolarity following the collapse of the Soviet Union,[43] or the possible shift back to multipolarity with the technologically driven rise of China on the world stage. Key organizing concepts in international affairs include sovereignty, security, anarchy, etc. For instance, the proliferation of nuclear weapons has changed notions of security and how states can achieve it.[44] Finally, Weiss lists nine sub-categories that serve as a lens through which to understand how technology changes relationships between international actors:

> (i) reordering hierarchies of military power, (ii) reordering hierarchies of economic power, (iii) redefining international economic relations, (iv) creating or resolving international problems, (v) creating new resources, (vi) creating new coalitions, (vii) creating new tools for international collaboration and (viii) creating new arenas for cooperation and competition. (ix) The relations among nations may also be influenced by the processes of professional cooperation and communication among scientists in different countries.[45]

The potential to reorder the balance of military power (number (i)) has been the focus of much of the debate and policy action when it comes to AI in international affairs. In the U.S., DoD has been a first mover in implementing AI as well as developing policy to govern its use. It recently established the Joint Artificial Intelligence Center (JAIC) to focus and coordinate its AI strategy, which includes [l]eading in military ethics and AI safety.[46] Several leading think tanks have also written excellent analyses of the implications of AI for national security through military and intelligence gathering uses.[47] The worry is that AI will enhance the military's efficiency and ability to respond to threats (i.e. its operational processes) so much that any nation that does not implement it will be left in the dust.[48]

Foreign policy circles have similar concerns about the economic impact of AI (number (ii)). America's status as the largest economy in the world and a leading technological innovator are key to its status as a world power. If AI is as economically transformative as some experts claim,[49] then the economy that is able to develop and harness it will capture a massive competitive edge.[50] Worries about both military and economic competition with rival states, particularly China, appear to have shaped the Trump administration's recent "Executive Order

---

[43] *Id.*
[44] Weiss at 302.
[45] Weiss at 303.
[46] Summary of the 2018 Department of Defense Artificial Intelligence Strategy at 8.
[47] Ben Scott, Stefan Heumann, & Philippe Lorenz, *Artificial Intelligence and Foreign Policy*, STIFTUNG NEUE VERANTWORTUNG (2018); William A. Carter, Emma Kinnucan, & Josh Elliot, *A National Machine Intelligence Strategy for the United States*, CENTER FOR STRATEGIC & INT'L STUDIES (2018); Michael C. Horowitz, Gregory C. Allen, Edoardo Saravalle, Anthony Cho, Kara Frederick, & Paul Scharre, *Artificial Intelligence and International Security*, CENTER FOR NEW AM. SECURITY (2018); Patrick Lin, George Bekey, Keith Abney, Autonomous Military Robotics: Risk, Ethics, and Design (2008); Greg Allan, Taniel Chan, Artificial Intelligence and National Security, Belfer Center for Science and International Affairs (2017).
[48] Michael C. Horowitz, *The Algorithms of August*, Foreign Policy 30 (Fall 2018).
[49] https://www.gsb.stanford.edu/insights/andrew-ng-why-ai-new-electricity; https://www.theverge.com/2018/1/19/16911354/google-ceo-sundar-pichai-ai-artificial-intelligence-fire-electricity-jobs-cancer.
[50] Kai-fu Li, AI Superpowers.

on Maintaining American Leadership in Artificial Intelligence."[51] The order makes frequent reference to "American AI," and directs certain programs to give preference to American citizens in funding, education, and workforce development.[52]

AI's contribution to America's military and economic power relative to other nations is an important issue, and narratives about an AI's "race" akin to the nuclear or space race have motivated policy makers to finally act. However, as Professor Weiss's framework shows, military and economic races are just two facets of only one *category* of AI's impact on international affairs. For instance, consider how AI could create new strategic resources, or create or strengthen international coalitions. Modern machine learning techniques require large amounts of both computing power (a.k.a. compute) and data. The Trump EO recognizes this implicitly when it directs agencies to open their data for private sector use, but it does not appear to approach this topic in a systematic way. Meanwhile, policy action in Europe and the U.S. reveal democratic states may be of like-mind when it comes to ensuring fairness, transparency, and accountability of algorithms and AI.[53] These shared values could lead to broader cooperation in AI and technology governance.

A narrow focus also ignores the potential changes to the structure and key organizing concepts of international affairs. Is technological competition inevitable, or are there opportunities for collaboration?[54] Does functionalism triumph over realism in a world where technology is embedded into more aspects of our daily lives, or does a move away from monopolarity create competing global systems that cannot interoperate? What is the role of extraterritorial policy making when technology transcends national borders?

3. Creating new issues areas, constraints, and tradeoffs

The third category of Professor Weiss relates to the substance of international affairs. He writes that science and technology impact substance by: "(1) creating new issue areas," "(2) creating new constraints and trade-offs in the operational environment of foreign policy," (3) creating "intermestic" issues where the line between international and domestic issues blurs, and "(4) changing the scope and domain of different paradigms of international relations theory."[55]

AI is itself already becoming a new issue area in international relations. The United Nations has convened meetings and is in the process of forming bodies to explore its implications.[56] Advocacy groups have also called for the creation of a new treaty restricting or banning LAWs.[57] The proliferation of AI work by serious scholars and reputable think tanks like Brookings, CSIS, CNAS, and others is further evidence that AI is becoming its own issue area within international affairs. However it remains to be seen how much AI develops as its own field of study in

[51] https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/
[52] *Id.*
[53] GDPR, Trump EO, proposals in Washington State, others.
[54] https://www.brookings.edu/research/us-china-relations-in-the-age-of-artificial-intelligence/.
[55] Weiss at 300.
[56] http://www.unicri.it/in_focus/on/UNICRI_Centre_Artificial_Robotics
[57] https://www.stopkillerrobots.org/; https://www.icrac.net/.

international affairs, or if it remains inextricably linked to topics like privacy, the internet, and telecommunications policy.

Possible new constraints created by AI are difficult to predict, as the limits of this technology are not yet well understood. First, a definition. "Operational environment" is a term of art in foreign policy that describes external factors that define the universe of options from which a decision-maker might choose.[58] Professor Weiss cites environmental damage caused by climate change as the quintessential constraint created by science and technology.[59] Such changes in the actual environment would constrain the options (the operational environment) available to decision makers, and such environmental changes would themselves be caused by failure of the international system to act to curb carbon emissions. Some commenters have raised alarm that strong AI will pose an existential threat to humanity,[60] which would certainly change the operational environment, though other experts dismiss this scenario.

As AI becomes widespread, a number of domestic issues are likely to become "intermestic." Chief among them is the impact of automation on the labor market. Experts worry that job displaced from automation will cause economic upheaval that will turn into political upheaval.[61] Concerns about economic competition between the U.S. and rival powers like China might also fall into this category. So on the one hand, U.S. policy as expressed by President Trump's EO seeks to stimulate the pace of AI development in the U.S. to maintain America's economic leadership. On the other, AI may cause massive economic disruption that further disrupts both domestic and global political systems. A comprehensive AI strategy must prepare for both outcomes. There are also many unknowns about how AI and automation will change existing niches in the global trading system. Low skilled, low cost manufacturing has traditionally been a pathway to jobs and growth in the global south, but widespread automation could change that pattern.[62]

Privacy and data policy is another area that is already intermestic to a degree and will likely become more so with AI. At the 2019 World Economic Forum at Davos, Japanese Prime Minister Shinzo Abe called for an increase in global data flows to facilitate the development of AI.[63] Yet recent litigation over Privacy Shield and the GDPR demonstrate that international data flows are not a given. In fact, many aspects of technology policy have taken on an increasingly international flavor as American tech companies have extended their reach globally, and this trend is likely to accelerate with AI. Some commenters, particularly tech companies themselves, have sought to position themselves as national champions in a global AI race as an argument against more vigorous antitrust enforcement.[64] Tech firms also worry that export controls and increased scrutiny from CFIUS will dampen foreign investment and slow AI development.[65]

---

[58] See Weiss, endnote 25; see also Hyam Gold, https://www.jstor.org/stable/2600167?seq=2#metadata_info_tab_contents;
[59] Weiss at 301.
[60] Cite
[61] CNAS. Many experts blame the rise in populism that propelled both Brexit and Donald Trump on similar economic factors. Cite.
[62] https://www.cgdev.org/publication/automation-ai-and-emerging-economies
[63] Cite
[64] Tim Wu article
[65] Cite NYTimes article.

AI policy issues that are currently examined mainly through a domestic lens will also become intermestic as AI plays a bigger role in international affairs. A growing body of scholarship and popular writing documents concerns over algorithmic bias and the need to develop AI tools that are fair, accountable, and transparent (FAT).[66] Legal scholars have written about how algorithms might be made to comport with the rigors of due process in the American legal system, for instance.[67] The desire for FAT AI will likely extend into the international arena, [68] but the legal rules and standards will be different. There is general agreement that at least in most areas of law, the U.S. Constitution only applies to U.S. persons.[69] Also, as domestic needs differ from foreign policy ones, the tolerances afforded in an international setting may also be different. Which set of rules should even apply? International human rights law is one possibility;[70] reliance on a technical standard set by a body such as the IEEE is another. It is at least plausible that the needs of a hypothetical facial recognition algorithm used at a U.S. embassy in Nigeria will differ from those at an airport in Seattle, or a government building in Wisconsin. If AI is used to make intelligence assessments or for strategic planning, how can those systems be validated? Is the standard for accountability lower because there is no express legal authority such as the FCRA, or higher because of the national security implications of an error?

Reliability/safety is another topic that is important in both domestic and international affairs, but will differ based on the context. The DoD's requirements for reliability may higher when it deploys an AV in a combat zone than when Waymo operates a robo-taxi in Chandler, AZ. Domestic safety standards may cause trouble as technology moves across borders if they are not interoperable. To return to an automobile example, does an AV need to have a software update before it can cross the border from Canada into the U.S.?

It remains far from clear how AI will change the underlying theoretical paradigms of international relations; such changes may only be fully understood in hindsight. However, the technical nature of AI suggests that it could continue to place an emphasis on international technical cooperation and standard setting, i.e. functionalism. Whether such technical cooperation will lead to cooperation in other arenas, as functionalist theory predicts, is yet unknown, however some commenters are already calling for the U.S. and China to find ways to work together.

4. Changing perceptions and information flows

The final category of Professor Weiss' framework is the way technology (1) alters perceptions, (2) serves as a source of information, and (3) provides new concepts and metaphors in international relations theory.[71]

[66] Ryan Calo, AI Policy Primer, UC Davis L Rev.
[67] Selbst and Boracas, others.
[68] https://tech.newstatesman.com/emerging-technologies/govtech-summit-justin-trudeau-ai-canada-china
[69] Swire, Woo, Desai, Hoover Article.
[70] https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf
[71] Weiss at 304.

One of the most worrisome ways that AI will likely change perceptions in international affairs is by facilitating political disinformation campaigns. First, AI that can generate text that appears to be written by a human could create fake news stories at an unprecedented rate. In the 2016 U.S. presidential election, large numbers of fake news stories written by humans are thought to have impacted public perception of the candidates. They did this in part by overwhelming the ability of social media users to and traditional media to fact check stories. If an AI is able to do the same while tirelessly and constantly iterating to create more effective stories, the scale of the problem would increase dramatically. In fact, a news story writing algorithm developed by the nonprofit OpenAI was so proficient that the group withheld part of its research because of "safety and security concerns."[72] The fake news problem could be even worse with the use of "deep fakes," AI powered videos that have been altered to make a real life person say and do things that they never done or said in real life. This technology is easily available on the internet and has created convincing fakes of Presidents Obama and Trump that are complete fabrications.[73] Currently, deep fakes often have subtle imperfections that give away their true nature, but the technology is rapidly improving.

AI could also be used to target and tailor messaging to individuals, improving the effectiveness of both fake news and genuine political communication. One of the main reasons that major tech companies invested so heavily in ML in the first place is to better target users for advertising. This micro-targeting was used in political process (apparently to great effect) by the now defunct Cambridge Analytica. Cambridge Analytica developed a way to profile individuals based on very specific psychological characteristics and target them with very specific political messages.[74]

This technology could also alter perceptions in ways completely unrelated to information warfare, of course. One of the main concerns cited by opponents of LAWs is that they could lower the perceived cost of going to war, which would ultimately lower the threshold for military conflict.[75] The narrative of an AI race between the U.S. and China may feed back into nationalist rhetoric on both sides, or AI powered tech companies like Facebook could help connect the world to an unprecedented extent.

AI may serve as a new source of information, or at least provide new insights from raw data that were previously unavailable. I have previously discussed how governments, the U.S. military in particular, intend to use AI to better analyze the vast amount of data available to them. For instance, AI has the potential to greatly improve analysis of satellite images.[76]

[Transition]

B. The Issue Areas for AI in IA

[72] https://slate.com/technology/2019/02/openai-gpt2-text-generating-algorithm-ai-dangerous.html
[73] https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peele-buzzfeed; https://www.cnbc.com/2018/12/07/deepfake-ai-trump-impersonator-highlights-election-fake-news-threat.html.
[74] https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win.
[75] Cite.
[76] https://www.technologyreview.com/s/611198/the-machine-vision-challenge-to-better-analyze-satellite-images-of-earth/.

By organizing the different areas of influence of AI in international affairs, the proceeding section sought to give a fuller accounting of this topic than has come before. Much of the discussion has focused on AI development could change the balance of power between the U.S. and China, either in military capabilities or their respective economic might. This section will synthesize some of the issues identified in the previous section in hopes of building a research agenda for AI in international affairs.

Military use of AI

The DoD's large budget and foresight on AI use relative to the rest of the government is likely to make it a leader in developing AI policy. At the same time, the military has unique needs that are distinct from those of the private sector and even other areas of government. Thus, its use of AI warrants particularly thorough investigation. One of the chief tasks for the DoD's AI policy experts is to develop rules governing autonomous weapons and the role of humans in the loop. Should autonomous weapons be used be employed offensively or defensively? In which aspects a weapons system can AI be deployed safely and effectively? Advocates have called for a human to be in the loop for any use of lethal force, but will competition with China or Russia push the U.S. toward LAWs? What is the potential for deskilling in warfare thanks to AI?

The military also needs to consider its procurement processes, its relationship with Silicon Valley, and AI workforce development. In recent years the DoD has sought to streamline its procurement processes to better keep with the pace of technological innovation.[77] This has involved efforts to purchase more commercially available tools instead of developing them in-house, and to work more closely with new technology companies. However, when Google employees forced the company to drop out of the military's Project Maven, it laid bare the culture gap between West Coast techies and the military establishment in Washington D.C.[78] The military and intelligence community will likely seek to build up their own talent pools, but the fact remains that they will need to rely heavily on the private sector for the foreseeable future.[79]

The details of the military's AI implementation will also be important, as the military has unique needs for reliability, safety, and security. It will need to determine where to set standards for reliability and safety, and those standards will likely be higher than in a civilian context, at least in some uses. What kind of audit procedures will be used for AI that makes targeting decisions? What does explainability mean for an AI that analyzes intelligence that will be used in strategic planning? Increased reliance on AI also presents a host of cybersecurity issues. First, more cyber-physical systems means a greater attack surface. AI presents novel security vulnerabilities that researchers are only just beginning to understand.[80] These requirements may complicate the procurement issues mentioned above.

Civilian Government Implementation

[77] https://www.washingtonpost.com/news/the-switch/wp/2016/06/10/the-pentagon-wants-to-cozy-up-to-silicon-valley-heres-one-big-thing-keeping-them-apart/?utm_term=.ef2f6119908b.
[78] https://www.nytimes.com/2019/03/01/business/ethics-artificial-intelligence.html?smid=nytcore-ios-share.
[79] https://foreignpolicy.com/2018/09/12/why-the-military-must-learn-to-love-silicon-valley-pentagon-google-amazon/.
[80] Is tricking a robot hacking?

The U.S. military's leadership in AI implementation is so stark in part because other sectors of the federal administrative state have lagged so far behind. The civilian arms of the federal government will need to work hard to truly become leaders in an "American AI Initiative"[81] Agencies like the State Department should consider the strengths of current AI techniques carefully, such as pattern recognition and problems with definable outcomes. Then, they should focus on the processes that could benefit most from AI while being subject to close scrutiny and pilot testing. The most promising processes for automation are those that have been proven in the private sector and have a clear analogue in the government. Fraud detection for financial crimes or sanctions evasion is a possible candidate,[82] as is predictive analytics for humanitarian relief.[83] By focusing on the processes by which international affairs operates, agencies can test discrete pilot programs informed by evidence-based policy making while maximizing impact for successful projects. This approach is preferable to dramatic overhauls that lack leadership and ultimately may waste taxpayer money.[84] Government IT procurement will also present a significant challenge. This is not a new challenge,[85] but this detail is crucial to effectively deploying AI in international affairs. Agencies can hardly rush toward adopting AI when they are running on decades old legacy systems.[86]

The government will need to grapple with algorithmic bias and fairness in AI, though the flavor of these issues will likely be different from those in the private sector. More work is needed to understand how AI fits into the existing international human rights regime. Policy makers must decide what level of accountability and fairness is required for the unique missions and constraints of international affairs.

International Competition in AI

U.S. competition with foreign States, particularly China, has driven much of the narrative around AI in international affairs thus far. It is a central theme in Trump's "American AI Initiative."[87] My goal is not necessarily to change this narrative on my own, but rather to open the eyes of policy makers to the full scope of AI's influence in international affairs. To the extent that framing AI as a race reduces complacency at the federal level or drives funding for basic science, it may well be a good thing. So far, the Trump administration's main policy initiatives have focused on "protecting our technological advantage in AI and protecting our critical AI technologies from acquisition by strategic competitors and adversarial nations."[88] Specifically, the administration pushed for and got legislation reforming CFIUS to scrutinize

[81] https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/
[82] https://www.thebanker.com/Transactions-Technology/AI-and-the-new-age-of-fraud-detection?ct=true.
[83] https://blogs.microsoft.com/on-the-issues/2018/09/24/using-ai-to-help-save-lives/.
[84] https://www.politico.com/story/2018/04/05/tillerson-state-department-consultants-503557
[85] https://www.washingtonpost.com/news/the-switch/wp/2015/03/13/the-state-departments-cyber-infrastructure-is-in-need-of-an-overhaul/?utm_term=.53c7eba3493c; https://www.aspanet.org/ASPADocs/Annual%20Conference/2018/Papers/PegnatoJoe.pdf.
[86] https://www.networkworld.com/article/3075358/not-dead-yet-7-of-the-oldest-federal-it-systems-still-wheezing-away.html.
[87] https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.
[88] Trump EO §1 (e).

foreign acquisitions of critical technologies like AI and is exploring export controls for AI and other emerging technologies. This paper takes no position on these policy actions other than they will likely be insufficient in themselves to preserve the preeminence of "American AI." Experts have lamented the repeated cuts to long term, basic science research that undergirds advances in AI.[89] While the Trump administration's commitment to greater funding as expressed in his Executive Order are encouraging, the lack of specificity does not inspire confidence. Even if China's falls short of its $147 billion goal for AI funding, the number signals the country's commitment to AI dominance and the specific steps they are willing to take to achieve it.

Information Security/Fake News

With revelations of Russian interference in the 2016 and 2018 elections, there is a growing recognition that nations are information systems, and democracies are vulnerable to certain types of information attacks.[90] Such attacks are not likely to end anytime soon. Technologies like AI that can drastically alter perceptions and change the way individuals receive or process information will play a large role in these kinds of attacks. Proposed countermeasures include automated detection, mandatory disclosure, information sharing, and civics education.[91] There is likely no one silver bullet. However, the actions of OpenAI in not releasing the full model of its news text generating AI raises questions of tech firms in accounting for the possible harms of their technologies. If the digital commons becomes polluted with the negative externalities of emerging technologies (i.e. fake news), is there a way for policy to prevent firms from socializing those costs? Perhaps a company that develops an AI capable of writing fake news should also develop the detection model under a polluter pays principle akin to the superfund.[92] Such a proposal is likely to be controversial, but the broader takeaway is that grave threats require exploring uncharted policy waters for effective solutions.

Worker Displacement and Labor Policy

Job losses to automation and the "future of work" in the wake of AI have captured a great deal of popular and scholarly attention in recent years.[93] Even those who believe AI will generate more jobs than it destroys recognize the potential for uneven gains in the economy.[94] Like other technological innovations, AI will create economic winners and losers, and those losers are often motivated to vote. Studies suggest that in at least some industries and regions, automation contributed as much if not more to manufacturing job losses than free trade.[95] As recent political events have shown, job losses and social disruption can also influence attitudes toward

---

[89] https://www.technologyreview.com/s/613010/why-ai-is-a-threat-to-democracyand-what-we-can-do-to-stop-it/; https://www.technologyreview.com/s/610379/heres-how-the-us-needs-to-prepare-for-the-age-of-artificial-intelligence/; Calo, AI Policy Primer.

[90] Farrell & Schneier, Common Knowledge Attacks on Democracies, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3273111.

[91] Information sharing: https://www.politico.com/magazine/story/2019/03/03/what-a-kamala-harris-meme-can-teach-us-about-fighting-fake-news-in-2020-225515. Cite others

[92] Thanks to Reid Pryzant of the Stanford CS Department for suggesting the polluter pays principle.

[93] Cite a trillion, zillion articles and conferences.

[94] Cite

[95] https://carnegieendowment.org/2018/12/10/how-trade-did-and-did-not-account-for-manufacturing-job-losses-pub-77794; the picture is complicated of course: https://www.foreignaffairs.com/articles/2018-09-07/automation-really-blame-lost-manufacturing-jobs.

immigration and immigrants. Policy makers must consider how disruptive job losses and resulting social changes will impact stability and national security. They must worry about more than just AI replacing humans one to one. AI powered firms that prevail in winner-take-all markets may be so powerful that they act as monopsonies, single buyers on the labor market, and use their market power to suppress wages and benefits.[96] Further, as discussed above automation of manufacturing jobs could disrupt the traditional pathway out of poverty for many developing nations. On the other hand, the rapid rise of data labeling jobs in China and the U.S. shows that it is possible that AI will open up new blue collar job opportunities, ones that could be offshored.[97]

The other half of the AI jobs picture is workforce development and how to ensure a robust pipeline of workers to build and implement AI systems. The federal government has what the CSIS calls an "AI workforce debt,"[98] a lack of both the technical and managerial skills required to implement AI. If AI is truly in the age of implementation then training more competent engineers and project managers may be more important than superstar PhDs from elite universities. [99] In many cases, when the U.S. lacked native technical talent it has imported it in the form of immigrants.[100] However, this strategy seems to conflict with the Trump administration's broader policy goals on immigration; his AI EO directs existing fellowship and service programs to prioritize American citizens.[101]

New International Agreements and Actors

AI-related technologies may become the subject of new international agreements, or may create new subject matter niches in existing ones. As discussed, there is a push for new agreements restricting or banning LAWs. There are also many open questions as to how AI fits into existing human rights treaties, especially the ICCPR. The Defense and State Departments have a clearly stated view on LAWs (too early to ban them),[102] but there does not appear to be any publicly available information setting out a U.S. position on AI and the ICCPR. Further, any international agreements on cross-border data policy will relate to AI. New international actors may also emerge thanks to AI, or existing ones may take on new roles. The United Nations (UN) has convened a High Level Panel on Digital Cooperation that includes many AI experts,[103] and the International Telecommunications Union has also been active in this space,[104] as has the EU.[105] Amy Webb has proposed a Global Alliance on Intelligence Automation (GAIA), a centralized, global body to harmonize different approaches to data collection and use and AI norms.[106] The U.S. must decide whether and how it wants to participate in such forums, and how it will

[96] Cite research linking labor monopsony and wage stagnation.
[97] https://motherboard.vice.com/en_us/article/7xyabb/china-ai-dominance-relies-on-young-data-labelers; https://towardsdatascience.com/the-invisible-workers-of-the-ai-era-c83735481ba.
[98] CSIS, Artificial Intelligence and National Security: The Importance of an AI Ecosystem, (2018).
[99] Lee, AI Superpowers
[100] Cite
[101] Trump EO §7
[102] https://www.lawfareblog.com/too-early-ban-us-and-uk-positions-lethal-autonomous-weapons-systems
[103] http://www.un.org/en/digital-cooperation-panel/.
[104] https://www.itu.int/en/ITU-T/AI/Pages/default.aspx.
[105] https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence.
[106] https://www.technologyreview.com/s/613010/why-ai-is-a-threat-to-democracyand-what-we-can-do-to-stop-it/.

position itself. Where do U.S. interests align with those of its allies and other countries, and how far is it willing to take its competition with China?

Authoritarian Uses of AI

How to curtail bad government uses of AI like mass surveillance? Sanctions? ICCPR?

Several countries are deploying AI in ways that violate privacy, civil liberties, and human rights. Facial recognition's potential to supercharge mass surveillance regimes is particularly worrying, and AI can be used to track people in other ways. Many commenters have sounded alarms about China's AI powered social credit system.[107] Though the social credit system fills a critical gap in China's existing consumer credit rating system,[108] it has also prevented millions of people from purchasing plane and train tickets in China.[109] Moreover, China is increasingly selling this technology to countries around the world,[110] including the U.S.[111] However, authoritarian AI does not simply mean Chinese AI; even Canada has engaged in some questionable uses of tracking and "risk assessments."[112]

Policy experts are just beginning to grapple with how to address this problem.[113] Will international law as expressed in treaties like the ICCPR be able prevent AI-driven mass surveillance? Should democratic countries develop some kind of sanctions regime? Or, as I argue, does extraterritoriality have some role to play? This technology is rapidly spreading throughout the world now, and the U.S. risks being left behind before it can formulate an adequate response. Moral leadership and soft power are certainly useful,[114] but more proactive measures will likely be required as well.

Privacy, Accountability, and Data Policy

Because data is so central to the ML techniques that power the latest AI advances, policies that impact the collection, use, and sharing of data will influence AI both domestically and internationally. U.S. policy makers must consider h to facilitate access to data in sufficient

---

[107] https://www.wired.com/story/mortal-danger-chinas-push-into-ai/?utm_campaign=cityfalcon&utm_medium=cityfalcon&utm_source=cityfalcon; https://www.albawaba.com/news/artificial-intelligence-isnt-agent-oppression-china-its-already-tool-1246590; https://www.wired.co.uk/article/china-social-credit-system-explained.

[108] Dai Li Social Credit Article

[109] https://www.scmp.com/economy/china-economy/article/2186606/chinas-social-credit-system-shows-its-teeth-banning-millions.

[110] https://slate.com/technology/2018/08/chinas-export-of-cutting-edge-surveillance-and-facial-recognition-technology-will-empower-authoritarians-worldwide.html; https://yellrobot.com/facial-recognition-cameras-rio-carnival-brazil/; https://slate.com/technology/2018/11/venezuela-china-zte-authoritarian-surveillance-social-control-tech.html; https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/;

[111] https://www.scmp.com/news/china/science/article/2181749/chinese-technology-helping-new-york-police-keep-closer-eye-united.

[112] https://motherboard.vice.com/en_us/article/kzdp5v/police-in-canada-are-tracking-peoples-negative-behavior-in-a-risk-database.

[113] https://slate.com/technology/2018/08/chinas-export-of-cutting-edge-surveillance-and-facial-recognition-technology-will-empower-authoritarians-worldwide.html.

[114] https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order.

quantity and quality while protecting "civil liberties, privacy, and American values," as the Trump administration puts it.[115] The move to open federal government data to the private sector was welcomed by experts,[116] but many American tech companies also have ambitions abroad. Policy makers need to think about cross-border data rules and how data norms impact relationships with trading partners. Some regions or countries (namely Europe) enforce stronger privacy and accountability measures than the U.S., while others are weaker. As a result, the U.S. has championed alternative, more flexible data sharing models to the GDPR such as the APEC Cross-Border Privacy Rules. Potential federal privacy legislation could change this dynamic.

At the moment, access to large data sets is crucial to ML, but privacy advocates worry that the narrative of U.S. competition with China will create a race to the bottom on data policy.[117] I share this worry, and so the rest of this paper seeks to outline how the U.S. and democratic allies can influence global rules and norms around data, and how more protective privacy and accountability rules can become an advantage in a strategic AI competition.

Part II. Extraterritoriality, and How Unilateral Action Can Influence Data Norms Abroad

Two related trends are relevant to the discussion of global AI norms. First is the increased relevance of global public goods, and second is the rise of non-consent based international rule making. The concept of a public good is borrowed from economics and refers to goods that are "non-excludable (no one can be excluded from the good's consumption) and non-rivalrous (the good's consumption does not reduce its availability to others)."[118] "Pure" public goods are relatively rare, but public goods analysis can still apply to "impure" public goods that have both a public and private character.[119] *Global* public goods are those whose benefits are "quasi-universal in terms of countries," so the entire global community benefits from their existence and enhancement rather than a single country.[120] They can also be perfectly or imperfectly global.[121] Perfectly global public goods apply to all countries.[122] Reduction of CO2 emissions to combat climate change is a classic example of a perfectly global public good. Even if the benefit does not accrue to all countries, a public good may be imperfectly global as long as it benefits more than just one country, region, or club.[123] In the globalized, interdependent international system that exists today, many of the world's most pressing problems relate to the creation of global public goods. Climate change mitigation, anti-terrorism, global antimonopoly policy, global disease control and numerous other goals can only be achieved through international cooperation. At the same time, the reliance on consent and consensus in traditional international

[115] Trump EO.
[116] Cite
[117] https://foreignpolicy.com/2018/08/14/the-data-arms-race-is-no-excuse-for-abandoning-privacy/.
[118] Gregory Shaffer, International Law and Global Public Goods in a Legal Pluralist World at 673.
[119] Inge Kaul, Isabelle Grunberg, & Marc Stern, Defining Global Public Goods, in Global Public Goods: International Cooperation in the 21st Century ed. Inge Kaul, Isabelle Grunberg, & Marc Stern at 4.
[120] Inge Kaul, Isabelle Grunberg, & Marc Stern, Defining Global Public Goods, in Global Public Goods: International Cooperation in the 21st Century ed. Inge Kaul, Isabelle Grunberg, & Marc Stern at 3.
[121] Kaul et al refers to this as purely or impurely global. *Id.* at 11.
[122] *Id.* at 11.
[123] *Id.* at 11.

law means that free riding, strategic holdouts, weakest links, and collective action problems have greatly hampered international efforts to achieve such goals.[124]

Nico Krisch documents how the decline of consent-based mechanisms (treaties and international laws) has led to a reliance on non-consent based models to achieve global public goods.[125] While noting that consent has been surprisingly resilient in the face of increased criticism,[126] he nonetheless finds that when dealing with global public goods, alternative mechanisms that are unilateral, extraterritorial, informal, and/or hierarchical have been favored.[127] For example, although attempts at establishing a multilateral mechanism to enforce global antitrust principles have been largely fruitless, unilateral enforcement by the U.S. and EU have at least partially successful in providing this public good.[128] Krisch argues that this tactic has worked in in antitrust because "[c]ompanies cannot typically afford to ignore the regulations of major markets that they seek to enter, and cannot efficiently divide their operations and tailor them to the regulatory requirements of particular jurisdictions; the potential result is a race to the top in which the strictest standards prevail overtime."[129]

Professor Jennifer Daskal has begun to explore how extraterritoriality is being used by strong States to influence international privacy standards. She has astutely pointed out that the recent legislative action in both the EU and U.S. represent efforts to unilaterally and extraterritorially impose their respective data norms.[130] She describes both the GDPR and the CLOUD Act as representing:

> "a new form of international rulemaking, but through the de facto operation of the market and the multinational corporations that operate across borders—rather than the more formal and mutually agreed upon process of treaty making amongst states or international organizations setting standards that impose obligations on participating states."

The CLOUD Act imposes certain privacy safeguards such as independent judicial review and requests that are particularized and based on "articulable and credible facts"[131] upon foreign law enforcement agencies making requests on U.S. companies. As the U.S. is home to most of dominant global internet platforms, it is able to dictate a higher privacy standard than currently exists in many countries.[132] She cites the U.K.'s adoption of new judicial review provisions in its domestic law as evidence of this impact.[133] From the European side, she cites the GDPR's requirement to appoint data protection officers in firms and implement "adequate safeguards" on data as extraterritorial effects.[134] In addition, the EU's restriction against transferring data to countries without adequate privacy protections resulted in the extension of the Judicial Redress

---

[124] Andrew T. Guzman, Against Consent, 52 Virginia J. Int'l L. 747 (2012).
[125] Nico Krisch, The Decay of Consent: International Law in an Age of Global Public Goods, Am. J. Int'l L (2014).
[126] Krisch at 26
[127] Krisch at 28-29.
[128] Krisch at 12-15.
[129] Krisch at 13.
[130] https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/
[131] Cite Cloud Act.
[132] https://www.lawfareblog.com/why-cloud-act-good-privacy-and-human-rights.
[133] https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/.
[134] Daskal, Borders and Bits at 232.

Act to EU citizens as well as PPD-28.[135] Of course, the CLOUD Act and GDPR are not the first or only examples of extraterritoriality. The U.S. has long used domestic law to combat corruption abroad by American companies and money laundering, for example.[136] However, the globalization of data, including criminal evidence in the case of the CLOUD Act, has driven these trends further.[137]

Daskal notes that when extraterritorial regulation is effective, "it can lead to harmonization of practices across borders and, perhaps, increased protections for all. When ineffective, however, it can yield a potentially destabilizing clash of norms and legal obligations—pushing practices in a direction that contradicts a state's own norms and values."[138] Further, relying on private firms to safeguard individual rights can lead to inconsistent enforcement and can be detrimental to democratic accountability.[139] Still, Daskal suggests that with the right transparency, notice requirements, and public-private partnership in standard setting, these problems could be mitigated.[140]

Building on the works of Krisch and Daskal, I argue that informational privacy, and the related concepts of fairness, accountability, and transparency in data processing, are global public goods.[141] Scholars have argued that the internet is a global public good,[142] and that privacy is a public good[143] or that the lack of privacy is otherwise like an environmental pollutant and should be regulated as such.[144] However I have not found any scholarship advancing the claim that privacy is a *global* public good. Many have argued that more privacy in the international system, and especially in the global internet, is a good thing, often using the language of human rights.[145] But a global public goods analysis allows for a more structured way to think about the role of extraterritoriality in creating a privacy race to the top. Recall that global public goods are non-rivalrous and non-excludable, and provide a benefit to the entire global community.

Privacy is non-rivalrous: in almost all cases, the fact that my information is private does not diminish your privacy.[146] Privacy is imperfectly non-excludable: a legal regime that affords privacy to a polity will generally provision it to members of the polity roughly equally because to

---

[135] Daskal, Borders and Bits at 233.
[136] Cite to Foreign Corrupt Practices Act and Money Laundering Control Act.
[137] https://www.lawfareblog.com/why-cross-border-government-requests-data-will-keep-becoming-more-important.
[138] *Id.* at 235.
[139] *Id.* at 235-7.
[140] *Id.* at 237-9
[141] Because privacy is not an immutable commodity, an economist would probably argue that it is not a public good in the strict technical sense. However, the same could be true of competition enforcement or anti-terrorism efforts, which are considered global public goods. Thus, I use the term as it has been adapted in the international law literature. Great apologies to my on-call economist Jan Whittington.
[142] Debora L. Sparr, The Public Space of Cyberspace in in Global Public Goods: International Cooperation in the 21st Century ed. Inge Kaul, Isabelle Grunberg, & Marc Stern.
[143] Joshua A.T. Fairfield & Christopher Engel, Privacy as a Public Good, 65 Duke L. J. 385 (2015).
[144] A. Michael Froomkin, Regulating Mass Surveillance as Privacy Pollutant: Learning from Environmental Impact Statements, 2015 U. Ill. L. Rev. 1713 (2015); Dennis D. Hirsch, Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law, 41 Georgia L. Rev. 1 (2006).
[145] Cite shit-ton of stuff.
[146] There could be rare cases where different aspects of privacy conflict with one another, for example where individual anonymity interferes with the overall information security of a system.

do otherwise would entail political and social costs.[147] For instance, the 4th Amendment protections of the U.S. Constitution apply to U.S. *persons*, which includes lawful permanent residents and U.S. citizens abroad, not just U.S. citizens.[148] Note that I refer to privacy created in a system by formal legal rules and norms, not the privacy that results from individual choices to disclose or withhold information absent some legal guidance. Joshua Fairfield and Christopher Engel tackle this problem by conceptualizing a lack of privacy as a public *bad* and documenting the various negative externalities of that public bad.[149] Because a lack of privacy is a public bad, they conclude that privacy itself must be a public good.[150] They also conclude, as I do, that privacy is likely an impure public good.[151]

The benefits of informational privacy are well-trodden territory and too numerous to recount here.[152] [These concepts need to be expanded and applied to FAT algorithms, expand on this later]. If the international system had strong privacy rules, every person would at least have the potential to benefit from that system. There would be some individual variation; the shareholders of ad-reliant technology firms might suffer financially even though they would benefit from a privacy perspective. Citizens of nations with less developed ICT infrastructure or internet penetration would benefit less from a privacy perspective, but they would at least have the potential to benefit if and when they have access to the right technology. Also, certain nations that have benefited from lax privacy regimes would suffer, but that is the very nature of why the consent-based international system inhibits global public goods. All this means that just as privacy is likely an imperfect public good, it is also probably an imperfectly global public good. Still an international system of stronger international privacy rules would benefit people in a broad range of countries.

Krisch and Daskal show that old methods of consent-based international law are breaking down, and States may be able to use extraterritoriality to promote global public goods. I caution though that extraterritoriality is just one tool that has become increasingly prominent in the international rulemaking system. The U.S., EU, or any other country or bloc will not be able to simply impose its will through only unilateral action. Rather, I want to emphasize that certain global public goods are also in the U.S. national interest, and can be pursued using extraterritoriality.[153] The U.S. can and should pursue multilateral strategies and coordinate with allies where possible.[154] In Part III, I argue that strong privacy rules with the right extraterritorial effects could actually help the U.S. in a strategic competition to dominate AI.

Part III.

---

[147] Inge Kaul, Isabelle Grunberg, & Marc Stern, Defining Global Public Goods, in Global Public Goods: International Cooperation in the 21st Century ed. Inge Kaul, Isabelle Grunberg, & Marc Stern at 4. However, nations can and often do apply higher standards of privacy to their own polity as compared with non-members. Swire, Woo, and Desai, Hoover article.
[148] Swire, Woo, and Desai.
[149] Fairfield & Engel at 423-33.
[150] *Id.*
[151] *Id.* at 443.
[152] Cite metric shit-ton of stuff.
[153] Joseph S. Nye, The American Interest and Global Public Goods, 78 Intl Affairs 233 (2003).
[154] *Id.*

A. The framing of the AI race between China and the U.S.

The idea that China and the U.S. are racing one another to develop and widely implement AI is part of a broader narrative about competition between the world's current economic and military super power and a rapidly growing challenger. Competition over AI is one issue in a conflict that also includes a trade war, intellectual property theft, and accusations of spying against Chinese companies.[155] Part of what spurred the focus on technology was the 2015 announcement by the Chinese government of plans to invest heavily in certain high tech manufacturing capabilities in such areas as robotics, aerospace, semiconductors, biopharmaceuticals, and more, called "Made in China 2025."[156] Although focused on increasing China's domestic manufacturing capacity, the plan still provoked western anxiety of China's growing economic strength generally and in high technology specifically.[157] Made in China 2025 was followed in 2017 by an announcement that China planned to catch up to rival countries in AI by 2020, and to become a world leader by 2030.[158] These ambitions were backed by large monetary commitments to research and development, at a time when the U.S. was cutting funding for science research.[159] Even though China has backed off its public promotion of Made in China 2025 and called for greater collaboration on AI, anxiety on the U.S. side remains high.[160] This anxiety can be seen in the title of President Trump's EO on AI, "Maintaining American Leadership in Artificial Intelligence," and the provision calling for the U.S. to

> promote an international environment that supports American AI research and innovation and opens markets for American AI industries, while protecting our technological advantage in AI and protecting our critical AI technologies from acquisition by strategic competitors and adversarial nations.[161]

Leading think tanks and scholars have promoted this narrative of AI competition with China and urged the U.S. to formulate national strategy for AI.[162] There was a sense that the U.S. risked falling behind, as several other countries beside China has also created their own national strategies.[163] The President finally took the first step in February of 2019 with his Executive Order, and the military published a summary of its strategy shortly after.[164] To the extent that this AI race narrative has spurred the federal government from complacency into new policy action and investment in AI, it is a positive thing.

If the policy levers being employed by the Trump administration are an indication, high level U.S. policy makers have bought into this race narrative. The administration's key measures on

---

[155] Cite.
[156] https://www.csis.org/analysis/made-china-2025.
[157] https://www.china-briefing.com/news/made-in-china-2025-explained/.
[158] https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html.
[159] https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html.
[160] https://www.scmp.com/tech/policy/article/2188732/beijing-increase-support-manufacturing-upgrade-even-though-made-china; https://www.technologyreview.com/s/612141/chinas-leaders-are-calling-for-international-collaboration-on-ai/
[161] Trump AI EO.
[162] Cite.
[163] Cite France, Canada, Japan, etc.
[164] Cite.

AI and international affairs so far have been to push for CFIUS reform and export restrictions on emerging technologies, particularly AI. In 2018 Congress passed the Foreign Investment Risk Review Modernization Act (FIRRMA).[165] FIRRMA broadened CFIUS' jurisdiction in several important ways, including to cover "emerging and foundational technologies"[166] The bill's drafters were open about the fact that they were targeting Chinese acquisitions of American technology,[167] and many experts agreed that the legislation was necessary.[168] At the same time, some in Silicon Valley expressed concern about FIRRMA's additional regulatory complexity.[169] Many of the details for how to protect America's national security interest in its emerging and foundational technologies were left to the Commerce Department, and Treasury has issued interim regulations.[170]

The other recently enacted tool to combat China in a global AI competition is Export Control Act of 2018.[171] Commerce began the rulemaking process later that year.[172] While there was wide agreement that FIRRMA was necessary and useful, if difficult to implement in actual practice, export controls have been more controversial. Silicon Valley entrepreneurs worry that the restrictions will hurt their ability to enter new markets, hire talent, or otherwise harm their competitiveness.[173] Georgia Tech Professor Mark Riedl points out that the algorithms that make up ML are basically complex math equations, so it will be very difficult to draw a line around what constitutes AI for regulatory purposes.[174]

Both CFIUS Reform and restrictive export controls seem to fit with the Trump Administration's broader economic nationalist stance. Recall that the Trump AI EO specifically called for "protecting our technological advantage in AI and protecting our critical AI technologies from acquisition by strategic competitors and adversarial nations."[175] That order also made a point to reserve funds and programs for U.S. citizens where possible.[176] However, it did not set specific funding numbers for AI or basic science research. The Trump administration's proposed budget for 2020 called for increased spending in civilian and military AI research and deployment, but

---

[165] https://home.treasury.gov/sites/default/files/2018-08/The-Foreign-Investment-Risk-Review-Modernization-Act-of-2018-FIRRMA_0.pdf.
[166] FIRRMA 1703(a)(6).
[167] https://thehill.com/blogs/congress-blog/technology/379621-firrma-act-will-give-committee-on-foreign-investment-a-needed.
[168] https://www.lawfareblog.com/innovation-security-conundrum-us-china-relations; https://www.csis.org/analysis/investment-restrictions-china-decision-wasnt; https://www.cfr.org/blog/cfius-reform-not-solution-start.
[169] https://techcrunch.com/2018/08/17/a-new-foreign-investment-bill-will-impact-venture-capital-and-the-u-s-startup-ecosystem/.
[170] https://home.treasury.gov/news/press-releases/sm506.
[171] https://www.congress.gov/bill/115th-congress/house-bill/5040/text?format=txt.
[172] https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies.
[173] https://www.nytimes.com/2019/01/01/technology/artificial-intelligence-export-restrictions.html; https://www.technologyreview.com/s/612453/a-us-attempt-to-keep-ai-out-of-chinas-hands-could-actually-help-china/; https://www.scmp.com/news/world/united-states-canada/article/2174229/us-restrict-foreign-investments-ai-biotech-curbing.
[174] https://medium.com/@mark_riedl/us-export-control-of-artificial-intelligence-research-considered-harmful-fb2986fb3f14.
[175] Trump AI EO.
[176] Cite.

also cuts to the National Science Foundation, the main government funder of scientific research.[177] So it appears that technological competition with China is pushing the Trump administration to action, albeit in an uneven manner.

However, some commenters fear that this narrative will generate a race to the bottom with regard to privacy and other regulatory guardrails on privacy.[178] This is because contemporary ML techniques require large amounts of data to function properly. Mark Zuckerberg has cautioned that to impose privacy regulation on American technology companies would inhibit their ability to compete with the Chinese tech giants with which we are competing.[179] At the same time, Kai-fu Lee has argued that China is the "Saudi Arabia of data," both because it has lax or ineffective privacy laws and because Chinese companies have insinuated themselves into the real lives of Chinese users.[180] Whereas American companies tend to stick to their online platforms, Chinese companies have made themselves vital to Chinese users who order food, pay rent, and generally run their lives through their smartphones.[181] The reasoning goes that if data is a vital resource for AI, and China has such a great advantage in data gathering, then any U.S. limits on data collection would only hobble American tech companies in their competition with China. This reasoning is seductive, but the purpose of this article is to suggest the opposite: that engineered correctly, international competition can result in a race to the top for certain global public goods like privacy and related concepts of fairness, accountability, and transparency.

B. How to Create a Privacy Race to the Top

- Analysis of previous U.S. extraterritorial action in antitrust and anti-corruption enforcement.
- U.S. enacts strong data privacy protections along with requirements that algorithms be fair, accountable, and transparent. At this point I'm agnostic on the exact provisions.
- This creates a club with strong privacy protections and FAT algorithms, and any companies wishing to access the markets in the club must comply.
- Use multilateral tools like APEC CBPR or Data Free Flow with Trust framework to expand the club. The more the club grows, the greater the incentive for other countries to implement privacy protections.
- Extraterritorial enforcement of privacy and FAT. If companies have to audits for bias, or demonstrate that their training data sets were compiled through means that comply with strict privacy standards, American and European companies may be better able to do that than Chinese ones.
- Also, sanctions or enforcement against companies that use AI to deliberately violate human rights. But there are a lot of difficult lines to draw here.

C. The Limits of Extraterritoriality

[177] A Budget for a Better America
[178] https://foreignpolicy.com/2018/08/14/the-data-arms-race-is-no-excuse-for-abandoning-privacy/
[179] https://foreignpolicy.com/2018/08/14/the-data-arms-race-is-no-excuse-for-abandoning-privacy/.
[180] Kai-fu Lee, AI Superpowers
[181] Lee, AI Superpowers.

- Lack of democratic accountability (Daskal)
- Hard to influence nations that are cut off globally, as the Chinese internet is. This strategy only works of Tencent, Alibaba, Baidu, et al want access to American and European markets.
- Could push toward fracturing of internet or other global institutions
- Could be used for anti-social purposes or by authoritarian states