FEBRUARY 2020

Recommendations on Export Controls for Artificial Intelligence

CSET Issue Brief

CSET
CENTER *for* SECURITY *and* EMERGING TECHNOLOGY

AUTHOR
Carrick Flynn

The U.S. government has recently begun to pay close attention to the export of artificial intelligence[1] and AI-relevant technologies.[2] In addition to AI's economic importance, it has a range of applications relevant to national security and human rights. [3] There are substantial national and global security risks if democratic nations lose their current lead in AI. Yet as the Department of Commerce has acknowledged, export controls are complicated policy tools that require the careful balancing of competing interests and priorities.[4]

This paper clarifies the stakes by reviewing and assessing options for export controls on AI software, algorithms, data sets, chips, and chip manufacturing equipment. The key takeaway is that chip manufacturing equipment is likely to be a highly effective point of export control, with other areas likely to be either ineffectual or affirmatively damaging to the interests of the United States and its democratic allies.

To summarize our findings more thoroughly:

- *New export control regulations on general purpose AI software, untrained algorithms, and datasets without military use are **unlikely to succeed** and **should not be implemented**.* Such regulations would potentially undermine U.S. competitiveness and damage the U.S. government's relationship with leading AI firms and the AI R&D community.

- *Highly application-specific AI software, trained algorithms, and militarily sensitive data sets **are useful targets** for export control, but **are already covered** by the current export control regime.* Natural extensions of current export control approaches targeting end uses and end users would cover existing and foreseeable export control needs in these areas. Enforcement is also likely to be easier than in the above cases, though still difficult.

- *Equipment for manufacturing AI chips **is likely a highly effective** point of export control.* Controls on such equipment effectively constrain who will be able to produce cutting-edge AI chips in the future. The design and production of such equipment requires advanced capabilities and rare expertise, and existing firms are based in a small number of democratic countries that are US allies.

- *The effectiveness of export controls on AI chips **will depend on** early implementation of export controls on chip manufacturing equipment. AI chips themselves **are not yet** a promising target for expanded regulation.* Export controls on AI chips without prior imposition of export controls on the equipment for manufacturing such chips will likely prompt targeted countries to invest in chip manufacturing capacity, achieve import substitution, and erode the supply chain advantage held by the United States and democratic allies.

Expanded export controls on general purpose AI software, untrained algorithms, and most datasets are unnecessary and likely counterproductive to U.S. leadership in AI

It is important to distinguish between "general purpose" and "application specific" AI software. When policy experts discuss "AI software," they are most often referring to general purpose AI software libraries built and open-sourced by private companies.[5] These libraries provide user-friendly frameworks for researchers, engineers, data scientists, and entrepreneurs to design and build application-specific AI software. General purpose AI software should not be conceptualized as a specialized tool, but as a "machinist shop" that can make specialized tools. It is also important to keep in mind that each of the specialized tools (application-specific AI software) made in this machinist shop can only serve a single, narrow purpose.

At the heart of AI software sit algorithms and methods—many that are decades old—published as "fundamental research." These general-purpose algorithms allow systems to "learn" how to complete a specific task by training them on specific data. Without specific data, which currently comes mostly in the form of enormous human-labelled datasets, training is not possible. Without training, these systems cannot do anything independently.

To summarize: general purpose AI software can be used to make application-specific AI software, which when trained on enormous amounts of specialized data, can complete very narrow tasks.

Innovation and competitiveness in AI rely on openness

Many of the most popular and important general purpose AI software libraries are built and open-sourced by U.S.-based private companies for commercial and competitive ends.[6] Some of the reasons why for-profit firms would incur the expense of developing software, only to offer it for free, include: benefiting from the free labor of open source developers, selling complementary products,[7] reducing the cost of training new employees through prior knowledge of the firm's software library, and generating goodwill, among others.

This open source ecosystem does not only benefit U.S. firms and their competitiveness; it also facilitates rapid diffusion and creates expert communities of tinkerers experimenting, iterating, and advancing the fundamental science and application of AI. The United States stands to reap substantial economic rewards as engineers, data scientists, and entrepreneurs use free machinist shops to craft the specialized parts and tools they need to fit their businesses' and industries' needs. Studies suggest this openness can be much more efficient and effective than a more closed system of development.[8]

These machinist shops, and the communities that have sprung up around them, exist online. By imposing export controls, the United States would effectively cede this powerful engine of innovation—and wealth generation—to other countries. It would also undermine the United States' ability to develop and disseminate technology domestically, since this is mostly done on the internet. It would be as though the rest of the world had access to Wikipedia while the AI R&D community in the United States was forced to mail encyclopedias to one another.

Overly broad export controls in this area will harm R&D and threaten U.S. leadership in AI

Historically, the United States has invested more heavily in AI than China—the largest contributions being made by private industry. Export controls on general purpose AI software, untrained algorithms, and most datasets would harm the profitability of the U.S. AI industry and shrink R&D investment. (In particular, compliance with export controls is likely to disproportionately harm small businesses and start-ups, whose innovation has been central to U.S. industry's success.) Meanwhile, the Chinese government plans to allocate billions of dollars to subsidize the development of AI technologies in China.[9] Were the U.S. government to undermine domestic R&D investment as the Chinese government dramatically subsidizes its AI industry, the U.S. would jeopardize its leadership in AI.

Export controls might also harm the U.S. AI workforce. If export controls restrict who can work on AI technologies in the United States, and what American researchers can share and discuss with non-American colleagues,[10] it will reduce the attractiveness of U.S. research organizations and companies to AI researchers from around the world. This will be a serious loss for Silicon Valley, where more than half of all technology workers are immigrants.[11] Among those immigrants are many of the world's top AI researchers. Furthermore, many American-born researchers prize the opportunity to work with the best researchers from around the globe. If export controls cause fewer world-class researchers to come to the United States and drive many to leave, U.S.-based AI firms would suffer, to the benefit of firms in other nations.

With the strongest technology companies drawing the brightest technical talent from around the world, AI leadership is America's to lose. Imposing export controls that damage our tech companies, reduce investment in R&D, and scare away our talent, is one way to do exactly that.

Export controls on AI software are likely to damage U.S. government partnerships with industry

The U.S. government could substantially damage its fragile relationship with U.S. AI firms by constraining their ability to share advances in AI research.[12] Many leading AI researchers are committed to sharing results, code, and data, even in cases that fall short of "fundamental research." Constraints on sharing could alienate a large fraction of the U.S. AI research community, with researchers unlikely to believe such an infringement is justified by legitimate national security considerations. Last year, an AI research non-profit refused to release one of its own trained models out of dual-use concerns.[13] This generated an outcry from the AI research community, despite the fact that they created the model and released the software and much of the dataset for the code.[14] As we have seen with Google's withdrawal from Project Maven and other examples of AI community activism,[15] there is a strained relationship between Silicon Valley and the U.S. government. Imposing additional regulations that are neither logical nor likely to be effective in practice, risks doing irreparable harm to this important relationship.

Export controls on general purpose AI software are unlikely to stop its spread

With some types of software, especially expensive proprietary software, firms have strong financial incentives to prevent piracy. Even in these cases, it is often difficult to do so, and software piracy is common. However, with general purpose AI software, not only is most of it already open-sourced and readily available to researchers around the world, firms actually want it to be open-sourced and as widely disseminated as possible. In these cases, firms are not incentivized to invest heavily in anti-piracy practices.

Export controls on narrow, application-specific AI software, trained algorithms, and dual-use datasets are appropriate but are covered by existing approaches

Application-specific AI software and trained algorithms can be controlled under the current Commerce Control List (CCL) where it covers "software that is specially designed for the development, production, or use of controlled commodities."[16] This could include application-specific AI software used for social control, censorship, and surveillance[17] as part of the CCL's regulation of "crime control and detection equipment, related technology and software."[18] Similarly, the specific data needed to train a general purpose algorithm into a narrow system that is militarily relevant is already covered by the munitions list.[19]

Narrow tailoring of regulations would inflict less economic damage, and has two additional advantages: 1) It will be easier, and 2) It might actually *improve* the relationship between the U.S. government and the AI research community.

Unlike general purpose AI software, where there is a financial incentive is to make it open source and as broadly adopted as possible, the incentive with application-specific AI software is to limit dissemination and protect it from piracy. The effort and expense to produce an effective application-specific AI system is substantial, and the profit comes from selling it directly as a final product. Palantir, for example, charges many thousands of dollars per user for its software and requires expensive updates.[20]

The AI R&D community is heavily populated by cosmopolitan civil libertarians[21] who care about preventing state oppression and militarism of the sort China increasingly practices.[22] Restricting export of application-specific AI software, unlike other types, could actually improve the relationship between the U.S. government and Silicon Valley by showing a commitment to shared values.

Export controls on AI chip manufacturing equipment *are* likely to be effective and should be a high priority

The computing power required for AI increasingly relies on specialized microprocessors, "AI chips," optimized for AI applications. AI chips are produced using highly advanced semiconductor manufacturing equipment that is relatively easy to define, monitor, track, and control.

Democratic nations have a virtual monopoly on the global market in semiconductor manufacturing equipment. A small number of firms in democratic nations produce the equipment, including firms based in the United States (47%), Japan (30%), the Netherlands (17%), South Korea (<3%), and Germany (<3%).[23] Some export controls for this equipment already exist,[24] though licenses are usually granted for the manufacturing equipment needed to produce chips a generation or two behind.[25] This amount of control has not prompted substantial import substitution, likely because of the difficulty and expense of producing this equipment.

China will have difficulty replicating, illicitly transferring, or stealing many necessary components of semiconductor manufacturing equipment. Photolithography equipment, for example, accounts for just one part of the process of making chips but presents a replicability challenge for China: only a few dozen units are produced each year by a single firm at a cost of $116 million per unit.[26] Even at this price, and with the most experienced experts in the world, the firm cannot produce the equipment at a pace matching demand and faces a substantial backlog.[27] Although this firm only produces photolithography equipment for chip making, it has a market capitalization of well over $100 billion—indicating the sophistication of this machinery.[28] Aside from photolithography equipment, other types of semiconductor manufacturing equipment similarly result from decades of production experience and billions of dollars in R&D, making them difficult to replicate. Moreover, the rarity, physical size, and financial stakes of these tools create additional challenges should China seek to circumvent export controls through illicit transfer or theft.

If semiconductor manufacturing equipment is export controlled, China will remain dependent on firms headquartered in the United States, Taiwan, South Korea, and Japan for its AI chips. Because China would rely on democratic states and traditional U.S. allies for an essential input, it would be constrained in how it develops and deploys its AI systems.

Increased export controls on AI chips at this time are likely to be counter productive

In the absence of stronger controls and stricter enforcement on semiconductor manufacturing equipment,[29] increased export controls on AI chips will only erode the important supply chain advantage of the United States and other democratic states. While carefully targeted end-use and end-user controls on chips may be appropriate, any broader controls on AI chips will likely encourage import substitution through the growth of an indigenous semiconductor industry. With end-use and end-user controls, the United States can continue to export chips while maintaining leverage to prevent these chips from threatening U.S. security or human rights. Moreover, it can achieve this while preserving the future influence that comes from maintaining its position in the supply chain.

To understand what can happen when chips are controlled but chip manufacturing equipment is not, consider the case of Xeon processors and the TaihuLight supercomputer. In 2016, when export controls prevented Intel from shipping Xeon processors to China for use in the Sunway TaihuLight supercomputer, China substituted in locally designed Sunway SW26010 processors. (These may have been made with semiconductor manufacturing equipment imported to China under BIS's Validated End-Users program.)[30] Less than a year and a half later, the TaihuLight was the fastest supercomputer in the world,[31] a title it held for two years. U.S. export controls on these chips provided significant technical experience and hundreds of millions of dollars of income for the Chinese microprocessor industry—income lost out on by Intel.[32] Export controls on AI chips are likely to prompt similar import substitution.

In conclusion

The United States can further global stability and human rights by keeping China's AI development and deployment reliant on the supply chains of democratic states into the foreseeable future. This can be achieved without impeding investment in U.S. AI R&D, and while perhaps even strengthening the relationship between the AI research community and the U.S. government. This requires a careful approach that pursues stringent controls on semiconductor manufacturing equipment and relatively narrow end-use and end-user controls on AI software, algorithms, data sets, and chips.

Acknowledgments

For their helpful discussions, comments, and input the author would like to thank Amanda Askell, Tessa Baker, Sue Gordon, Roxanne Heston, Andrew Imbrie, Saif Khan, Jade Leung, Jason Matheny, Kathryn Mecrow, Igor Mikolic-Torreira, Dewey Murdick, Tim Rudner, Helen Toner, Alexandra Vreeman, Lynne Weil, and Remco Zwetsloot.

References

Agarwal, Nityesh. “Examining the Transformer Architecture – Part 1: The OpenAI GPT 2 Controversy.” Exxact, 29 May 2019, https://blog.exxactcorp.com/transformer-architecture-part-1/.

astonished_crofty. “[Discussion] Should I release my MNIST model or keep it closed source fearing malicious use?” Reddit, 14 February 2019, https://www.reddit.com/r/MachineLearning/comments/aqovhz/discussion_should_i_release_my_mnist_model_or/.

Baldwin, Carliss, and Eric Von Hippel. "Modeling a paradigm shift: From producer innovation to user and open collaborative innovation." *Organization Science* 22, no. 6 (2011): 1399-1417.

Barrett, Brian. “China’s New Supercomputer Puts the US Even Further Behind.” *Wired*, 21 June 2016, https://www.wired.com/2016/06/fastest-supercomputer-sunway-taihulight/.

Bessen, James. "Open source software: Free provision of complex public goods." In *The economics of open source software development*, pp. 57-81. Elsevier, 2006.

Bitzer, Jürgen, and Philipp JH Schröder. "The impact of entry and competition by open source software on innovation activity." In *The economics of open source software development*, pp. 219-246. Elsevier, 2006.

Boudreau, Kevin J., and Karim R. Lakhani. "“Open” disclosure of innovations, incentives and follow-on reuse: Theory on processes of cumulative innovation and a field experiment in computational biology." *Research Policy* 44, no. 1 (2015): 4-19.

Broockman, David E., Greg F. Ferenstein, and Neil A. Malhotra. "Wealthy Elites’ Policy Preferences and Economic Inequality: The Case of Technology Entrepreneurs." *Working paper Stanford University* (2017).

Bughin, Jacques, Jeongmin Seong, James Manyika, Michael Chui, and Raoul Joshi. “Notes from the AI frontier: Modeling the impact of AI on the world economy.” McKinsey, Sept 2018, https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy.

Bureau of Industry and Security. “Commerce Control List.” Department of Commerce, 2018, https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl.

Cope, Sophia, Jillian York, Jeremy Gillula. “Industry Efforts to Censor Pro-Terrorism Online Content Pose Risks to Free Speech.” Electronic Frontier Foundation, 12 July 2017, https://www.eff.org/deeplinks/2017/07/industry-efforts-censor-pro-terrorism-online-content-pose-risks-free-speech.

Coren, Michael J. “More Silicon Valley tech workers were born outside the US than in it.” *Quartz*, 17 July 2017, https://qz.com/1029860/more-silicon-valley-tech-workers-were-born-outside-the-us-than-in-it/.

Defense Innovation Board. “Recommendations.” Department of Defense, 2017, https://innovation.defense.gov/Recommendations.

Department of Commerce. “Amendment to the Export Administration Regulations: Removal of Semiconductor Manufacturing International Corporation From the List of Validated End-Users in the People’s Republic of China.” *Federal Register* 81, no. 233 (December 5, 2016): https://www.bis.doc.gov/index.php/documents/regulations-docs/federal-register-notices/federal-register-2016/1611-81-fr-87426/file.

Department of Commerce. “Review of Controls for Certain Emerging Technologies.” *Federal Register* 83, no. 223 (November 19, 2018): https://www.govinfo.gov/content/pkg/FR-2018-11-19/pdf/2018-25221.pdf.

Ding, Jeffrey. *Deciphering China’s AI Dream: The context, components, capabilities, and consequences of China’s strategy to lead the world in AI.* Future of Humanity Institute, University of Oxford, 2018, https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf.

Flynn, Carrick. *Does China Have a National Security Relevant AI Data Advantage?* Center for Security and Emerging Technology, forthcoming.

Fryer-Biggs, Zachary. “Inside the Pentagon’s Plan to Win Over Silicon Valley’s AI Experts.” *Wired*, 21 Dec 2018, https://www.wired.com/story/inside-the-pentagons-plan-to-win-over-silicon-valleys-ai-experts/.

Future of Life Institute. "Autonomous weapons: an open letter from AI & robotics researchers." 2015, http://futureoflife.org/open-letter-autonomous-weapons.

Future of Life Institute. “Lethal Autonomous Weapons Pledge.” 2018, https://futureoflife.org/lethal-autonomous-weapons-pledge.

Knockel, Jeffrey, Lotus Ruan, Masashi Crete-Nishihata, and Ron Deibert. “ (Can’t} Picture This.” The Citizen Lab, 14 Aug 2018, https://citizenlab.ca/2018/08/cant-picture-this-an-analysis-of-image-filtering-on-wechat-moments

Lerner, Josh, and Jean Tirole. "The economics of technology sharing: Open source and beyond." *Journal of Economic Perspectives* 19, no. 2 (2005): 99-120.

Lewis, James. “Learning the Superior Techniques of the Barbarians: China’s Pursuit of Semiconductor Independence.” *Center for Strategic and International Studies*, January 2019, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190115_Lewis_Semiconductor_v6.pdf

Maurer, Stephen M. "The penguin and the cartel: Rethinking antitrust and innovation policy for the age of commercial open source." *Utah L. Rev.* (2012): 269.

McKenzie, John F. "US Export Controls on Internet Software Transactions." *The International Lawyer* (2010): 857-870.

Mozur, Paul. "Inside China's dystopian dreams: AI, shame and lots of cameras." *New York Times*, 1 July 2018, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

Nix, Naomi. "Google Drops Out of Pentagon's $10 Billion Cloud Competition." Bloomberg, 8 Oct 2018, https://www.bloomberg.com/news/articles/2018-10-08/google-drops-out-of-pentagon-s-10-billion-cloud-competition.

PwC. "China's impact on the semiconductor industry: 2016 update." 2017, https://www.pwc.com/gx/en/technology/chinas-impact-on-semiconductor-industry/assets/china-impact-of-the-semiconductor-industry-2016-update.pdf

Radford, Alec, Jeffrey Wu, Rewon Child, David Luan, Dario Amodei, and Ilya Sutskever. "Language models are unsupervised multitask learners." *OpenAI Blog* 1, no. 8 (2019). Available at: https://openai.com/blog/better-language-models.

Rao, Anand, Gerard Verweij, and Euan Cameron. "Sizing the Prize." PriceWaterhouseCoopers, 2017, https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf.

Raytheon Company. "Raytheon Company Comments BIS Emerging Technologies." 9 January 2019, https://www.regulations.gov/document?D=BIS-2018-0024-0077.

Rupp, Karl, and Siegfried Selberherr. "The economic limit to Moore's law." *IEEE Transactions on Semiconductor Manufacturing* 24.1 (2011): 1-4.

Semiconductor Manufacturing International Corporation. "2017 SMIC Corporate Social Responsibility Report." 2017, https://www.smics.com/uploads/2017%20SMIC%20CSR%20Report%20_EN.pdf

Shalf, John and Jim Ang. "SoC for HPC: An Agile Approach to Building HPC Systems from Commodity Components." *SoC for HPC*, 15 July 2016, http://www.socforhpc.org/wp-content/uploads/2015/04/AlternativeApproachToCommodityHPCv4.2.pdf.

Sun, Leo. "The U.S. Government Crushes Intel Corporation's Chinese Supercomputer Chip Sales." *The Motley Fool*, 15 Apr 2015, https://www.fool.com/investing/general/2015/04/15/the-us-government-crushes-intel-corporations-chine.aspx.

Tadjdeh, Yasmin. "China on Quest for Semiconductor Independence." *National Defense*, 12 April 2019, https://www.nationaldefensemagazine.org/articles/2019/4/12/algorithmic-warfare-china-on-quest-for-semiconductor-independence

Takahashi, Dean. "Globalfoundries: Next-generation chip factories will cost at least $10 billion." Venture Beat, 1 October 2017, https://venturebeat.com/2017/10/01/globalfoundries-next-generation-chip-factories-will-cost-at-least-10-billion.

Ting-Fang, Cheng. “Chinese chipmaker takes on TSMC and Intel with cutting-edge tool.” *Nikkei Asian Review,* 15 May 2018, https://asia.nikkei.com/Business/Companies/Chinese-chip-maker-invests-in-next-gen-tool-to-close-gaps-with-Intel-TSMC-Samsung.

US International Trade Administration. *2016 Top Markets Report Semiconductors and Semiconductor Manufacturing Equipment*. 2016, https://www.trade.gov/topmarkets/pdf/Semiconductors_Semiconductor_Manufacturing_Equipment.pdf.

Wang, Hanhan. “Palantir - Product or Services Company?” *Harvard Business School Digital Initiative*, 8 March 2015, https://www.hbs.edu/openforum/openforum.hbs.org/goto/challenge/understand-digital-transformation-of-business/palantir-product-or-services-company.html

Wassenaar Arrangement. "List of Dual-Use Goods and Technologies and Munitions List." 2018, https://www.wassenaar.org/app/uploads/2018/12/WA-DOC-18-PUB-001-Public-Docs-Vol-II-2018-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-18.pdf.

Wikipedia contributors, "List of semiconductor fabrication plants," *Wikipedia, The Free Encyclopedia*, https://en.wikipedia.org/w/index.php?title=List_of_semiconductor_fabrication_plants&oldid=904442735 (accessed July 16, 2019).

Zegart, Amy, and Kevin Childs. “The Divide Between Silicon Valley and Washington Is a National-Security Threat.” *The Atlantic*, 13 Dec 2018, https://www.theatlantic.com/ideas/archive/2018/12/growing-gulf-between-silicon-valley-and-washington/577963.

Zhang, Hugh. “OpenAI: Please Open Source Your Language Model.” *The Gradient*, 19 Feb 2019, https://thegradient.pub/openai-please-open-source-your-language-model.

Endnotes

[1] In this report, I am using the term "AI" to refer to artificial neural networks, though AI is a broader term that can also apply to other approaches.

[2] The *Export Control Reform Act of 2018* tasked the Department of Commerce (DOC) with considering export controls for emerging technologies (H.R. 5040, 115 Cong. 2018). The Bureau of Industry and Security (BIS) within the DOC then announced an advance notice of proposed rulemaking (ANPRM) indicating that they are considering export controls for AI and AI related technologies (Department of Commerce, 2018).

[3] Defense Innovation Board (2017). Flynn (forthcoming).

[4] From the ANPRM [see footnote 3]:

> *In identifying emerging and foundational technologies, the process must consider:*
>
> - *The development of emerging and foundational technologies in foreign countries;*
> - *The effect export controls may have on the development of such technologies in the United States; and*
> - *The effectiveness of export controls on limiting the proliferation of emerging and foundational technologies in foreign countries.*

[5] Examples include TensorFlow built by Google, PyTorch built by Facebook, and Microsoft Cognitive Toolkit.

[6] Lerner & Tirole (2004); Bessen (2005).

[7] One example would be Google selling access to "Tensor Processing Units" which are specialized chips specifically designed to work with TensorFlow.

[8] Baldwin & von Hippel (2011); Bitzer & Schröder (2016); Boudreau & Lakhani (2015); Maurer (2012).

[9] Ding (2018).

[10] Information does not actually have to leave the U.S. to be considered an export so long as a non-US national acquires it. This includes the acquisition of technical data. So if certain technical data is export controlled, providing potential access to this data by a non-citizen through, for example, working with them on a project, could be illegal. The term for this is a "deemed export." The effect of this is that non-Americans can be functionally barred from an industry if it includes a lot of export controlled technical data.

[11] Coren (2017).

[12] Fryer-Biggs (2018); Nix (2018); Zegart & Childs (2018).

[13] Radford et al. (2019).

[14] Zhang (2019); Agarwal (2019). For a sense of the depth of feeling this inspired there is an illustrative post and commentary on the Machine Learning forum (r/machinelearning) of the website Reddit titled "[Discussion] Should I release my MNIST model or keep it closed source fearing malicious use?" (astonished_crofty, 2019); Radford et al. (2019).

[15] Future of Life Institute (2015); Future of Life Institute (2018).

[16] McKenzie (2010).

[17] Cope et al. (2017); Knockel et al. (2018); Mozur (2018).

[18] 15 CFR § 742.7.

[19] "[T]here are existing controls impacting AI/ML such as controls on technical data and defense services under USML Category XI(d) directly related to defense articles under USML Category XI(a)(5)(i)" (Raytheon Company, 2019). And broadly 22 CFR § 121.1 where technical data is covered extensively.

[20] Palantir is not predominantly an AI company, but it is increasingly using these techniques. It is additionally an example of the type of firm producing sensitive proprietary software that would warrant export controls and where they likely would be relatively easy to enforce (Wang, 2015.)

[21] Broockman et al. (2017).

[22] Conversation with Dr. Amanda Askell, research scientist in ethics and policy at OpenAI.

[23] United States International Trade Administration (2016).

[24] These appear on the Wassenaar dual use list, which is an export control list agreed to by 42 countries, including all nations which export important pieces of chip production equipment—under category 3(B) (Wassenaar Arrangement, 2018). This also appears in the same category, 3(B), on the U.S. Commerce Control List (Bureau of Industry and Security, 2018.)

[25] The best example of past broad export licensing of this equipment to China comes from the Shanghai-based Semiconductor Manufacturing International Corporation (SMIC). SMIC is by far China's most advanced chip maker. Until 2016, SMIC was part of a special export license arrangement, called the Validated End-User Program (Department of Commerce, 2016) which allowed it to receive exports of U.S. semiconductor manufacturing equipment while circumventing the normal review process.

[26] Ting-Fang (2018).

[27] Schor (2019).

[28] The firm is ASML and it had a $130 billion market capitalization on the day this was written, 18 February 2020.
[29] Lewis (2019): Tadjdeh (2019).

[30] Which chipmaker produced these chips is unclear, but at least one source puts it as the Chinese-based SMIC (Shalf & Ang, 2016). Around this time SMIC also withdrew from BIS's Validated End User program (Department of Commerce, 2016.) SMIC imported much of its semiconductor manufacturing equipment from the United States (Semiconductor Manufacturing International Corporation, 2017). If SMIC did in fact use semiconductor manufacturing equipment imported from the United States to circumvent U.S. export controls on chips, this serves as an excellent example of why semiconductor manufacturing equipment is the essential point of control in this supply chain.

[31] Barrett (2016).

[32] Sun (2015).