AI Policy Levers: A Review of the U.S. Government's Tools to Shape AI Research, Development, and Deployment

Sophie-Charlotte Fischer, Jade Leung, Markus Anderljung, Cullen O'Keefe, Stefan Torges, Saif M. Khan, Ben Garfinkel, and Allan Dafoe[1]
Centre for the Governance of AI
Future of Humanity Institute, University of Oxford
March 2021
Centre for the Governance of AI, 2021: 10

read summary & conclusion

[1] **Acknowledgements:** We are grateful to the following people for their comments and discussion in shaping this report: Miles Brundage, Jeffrey Ding, Carrick Flynn, Matthijs Maas, Jason Matheny, Max Daniel, Alex Lintz, Luke Muehlhauser, Michael Page, Toby Shevlane, Helen Toner, and Brian Tse. We are particularly grateful for Remco Zwetsloot's help.

Cite as: Fischer, Sophie-Charlotte, Jade Leung, Markus Anderljung, Cullen O'Keefe, Saif M. Khan, Stefan Torges, Ben Garfinkel, and Allan Dafoe (2021): "AI Policy Levers: A Review of the U.S. Government's Tools to Shape AI Research, Development, and Deployment", #2021-10, Centre for the Governance of AI, Future of Humanity Institute, University of Oxford

Summary

The U.S. government (USG) has taken increasing interest in the national security implications of artificial intelligence (AI). In this report, we ask: Given its national security concerns, how might the USG attempt to influence AI research, development, and deployment—both within the U.S. and abroad? We provide an accessible overview of some of the USG's policy levers within the current legal framework. For each lever, we describe its origin and legislative basis as well as its past and current uses; we then assess the plausibility of its future application to AI technologies. In descending order of likelihood of use for explicit national security purposes, we cover the following policy levers: federal R&D spending, foreign investment restrictions, export controls, visa vetting, extended visa pathways, secrecy orders, prepublication screening procedures, the Defense Production Act, antitrust enforcement, and the "born secret doctrine."

The primary purpose of this report is to facilitate further research on the evolving role of the U.S. government in AI governance. We do not attempt a comprehensive normative assessment of the policy levers discussed, nor do we make policy recommendations. Our research for this report relied on publicly available sources and information provided by subject-matter experts.

Scope

We define *AI systems* as machines capable of sophisticated information processing.[2] This includes both systems developed using machine learning (ML) techniques and systems developed by researchers working within the "symbolic" or "good old fashioned AI" (GOFAI) paradigms. We define the broader category *AI technologies* to include both AI systems and computer hardware that enables the production and use of AI systems.

We focus on policy levers that are:

- *Domestic*, i.e., most directly constraining or supporting the activities of U.S.-based actors.[3]
- *Formal*, i.e., based on laws or other explicit government regulation, as opposed to informal sources of influence.
- *Direct,* as opposed to more indirect measures such as changing incentives provided by tax or intellectual property law, for example.
- *Based on existing legislation,* including for domains adjacent to AI that may come to apply to AI, as opposed to entirely novel influence mechanisms that might be introduced by new law.[4]

Our list is not exhaustive, and in the Conclusion, we point to additional levers that could be investigated in future work.

---

[2] Allan Dafoe, "AI Governance: A Research Agenda" (Oxford, UK: Governance of AI Program, Future of Humanity Institute, University of Oxford, 2018), 5, https://www.fhi.ox.ac.uk/wp-content/uploads/GovAI-Agenda.pdf.

[3] This excludes diplomacy, foreign intelligence collection, military operations, and other levers that most directly influence other states. It does include visa policies, foreign investment restrictions, and export controls, however, since these constrain the hiring, fundraising, and strategic decisions of U.S. firms.

[4] In particular, if there were sufficient national security concern, Congress could pass laws that significantly expand the USG's policy options, and executive wartime or crisis authority can be used to achieve much stronger levels of control. Consideration of these more extreme scenarios is beyond the scope of our analysis.

The Policy Levers: A Summary

Levers	Description	Potential Motives for Use	Key Decision-Makers	Likelihood of Use
Federal R&D Funding	Commissioning R&D projects and offering research grants	(1) Strengthen the domestic AI and semiconductor industries; (2) Make/keep relevant AI technologies available for national security purposes; (3) Gain insights into particular AI projects or the AI R&D landscape	National Science and Technology Council, Office of Management and Budget (among several actors who inform how federal R&D funding is allocated and spent)	Already in use. Further use likely.
Foreign Investment Restrictions	Limiting foreign investments in U.S. companies	(1) Undermine a rival's ability to use AI technology for national security purposes; (2) Deprive a rival of insights into particular AI projects or the AI R&D landscape	Committee on Foreign Investment in the United States (CFIUS) chaired by the U.S. secretary of treasury (including representatives from sixteen U.S. departments and agencies including Defense, State, Commerce, and Homeland Security); U.S. president	Already in use. Further use likely.
Export Controls	Limiting the export of particular technologies from the U.S.	(1) Undermine a rival's ability to use AI technologies for national security purposes; (2) Weaken the rival's AI and semiconductor industries	U.S. president; U.S. Trade Representative, Department of State, Department of Commerce (Bureau of Industry and Security); Department of Defense (Defense Technology Security Administration); Department of Energy; Department of the Treasury (Office of Foreign Assets Control); Member States of the Wassenaar Arrangement.	Already in use. Further use likely.
Visa Vetting	Limiting the number of visas awarded, particularly to students and workers in key industries	(1) Deprive a rival of insights into particular AI projects or the AI R&D landscape; (2) Undermine a rival's ability to use AI technologies for national security purposes	Department of Homeland Security, State Department	Already in use, to a limited extent. Further use plausible.
Expanded Visa Pathways	Increasing the number of visas awarded, particularly to workers in key industries	(1) Strengthen domestic AI and semiconductor industries; (2) Weaken a rival's AI and semiconductor industries	Department of Homeland Security, State Department	Major reforms unlikely. Targeted changes depend on the political climate & administration

Levers	Description	Potential Motives for Use	Key Decision-Makers	Likelihood of Use
Secrecy Orders	Preventing the disclosure of information in particular patent applications	(1) Deprive a rival of insights into particular AI projects or the AI R&D landscape; (2) Undermine a rival's ability to use AI technologies for national security purposes	U.S. Patent and Trademark Office, Defense agencies, U.S. president	There is some chance it is already in use in isolated cases. Extensive use is highly unlikely outside of national security crises.
Prepublication Screening Procedures	On a voluntary basis, screening papers for information that could be harmful to publish	(1) Deprive a rival of insights into particular AI projects or the AI R&D landscape (2) Undermine a rival's ability to use AI technology for national security purposes	National Science Foundation, Department of Defense, National Security Agency	Unlikely outside of substantial rise in national security concerns.
The Defense Production Act	Requiring private companies to provide products, materials, and services for "national defense"	Make/keep relevant AI technologies available for national security purposes	President of the United States, Department of Commerce (Bureau of Industry and Security), Department of Defense (Defense Production Act Title III Office)	Unlikely outside of substantial rise in national security concerns.
Antitrust Enforcement	Constraining the behavior of companies with significant market power; alternatively, refraining from these actions or merely threatening to take them	(1) Strengthen domestic AI and semiconductor industries; (2) Make/keep relevant AI technologies available for national security purposes	Department of Justice, Federal Trade Commission, private litigants, U.S. Supreme Court	Unlikely for uses directly motivated by national security concerns.
Born Secret Doctrine	Preemptively classifying all information relevant to the production of a particular class of technology	(1) Deprive a rival of insights into particular AI projects or the AI R&D landscape; (2) Undermine a rival's ability to use AI technologies for national security purposes	U.S. Department of Energy (unlikely to be the case if applied to AI)	Very unlikely outside of substantial rise in national security concerns.

Table 1: Summary of Levers

Federal R&D Funding

Since the Second World War, the USG has used federal funding as an instrument to promote technological development. In the domain of AI, the USG could use federal funding to advance domestic development or secure access to relevant intellectual property. The USG has many different funding mechanisms to support R&D. Some mechanisms, such as grantmaking by the National Science Foundation, confer little influence and access to the USG, while, for example, classified projects run by the Defense Advanced Research Projects Agency provide a great deal. The USG could also use defense procurement to develop specific AI systems or AI-relevant chips customized for national security applications. Notably, the USG has substantially increased its R&D funding for AI in the past few years, a trend that is likely to continue.

Foreign Investment Restrictions

The Committee on Foreign Investment in the United States (CFIUS) is an interagency body that reviews potential national security implications of foreign investments in U.S. companies and certain real estate transactions. In recent years, based on CFIUS recommendations, the president has already blocked several Chinese attempts to buy U.S. chip makers. In 2018, CFIUS's jurisdiction was significantly broadened through the Foreign Investment Risk Review Modernization Act (FIRRMA). FIRRMA expands, for example, the screening mechanism to also cover non-controlling investments that would allow a foreign entity access to critical technologies. While foreign investment restrictions might help to prevent the transfer of hardware technologies and early-stage developments in AI to some extent, they can also weaken the domestic industry by limiting its access to capital and foreign markets. The extent of future restrictions will depend on the perceived relative importance of these two effects.

Export Controls

Export controls restrict trade in order to prevent the cross-border flow of technologies and knowledge that present security concerns. The USG already applies export controls to some AI technologies, in addition to applying them widely across the semiconductor supply chain. Currently, the U.S. Department of Commerce is reviewing whether it should expand export controls under the Export Administration Regulations (EAR) to include additional AI technologies. The initial list of technologies under review for expansion is very broad and controls could significantly impact the business of American high-tech companies in foreign markets, as well as the operations of universities by restricting the access of foreign students and researchers to certain research projects. So far, the Commerce Department has only imposed new controls on a very small number of emerging technologies. It remains to be seen whether additional controls regarding AI and semiconductors will be issued.

Visa Vetting

The USG could use its visa vetting procedures for foreign AI researchers, students, and workers to deny perceived rivals access to sensitive technical information. The USG has increased its scrutiny of Chinese visa applicants working or studying in related fields over the past few years. While this lever might be effective in preventing some cases of espionage and technology transfer, it could also reduce the competitiveness of U.S. companies and universities by reducing their access to AI R&D talent.

Expanded Visa Pathways

The USG could expand and streamline existing visa programs or create new ones to recruit more foreign AI researchers and professionals, either to strengthen the domestic AI and semiconductor industries in general or to support specific projects relevant for national security. Such measures could address the existing skills gap in the domestic AI and semiconductor industries. However, they could also pose risks to U.S. national interests by enabling illicit technology transfer.

Secrecy Orders

The Invention Secrecy Act (1951) authorizes the U.S. Patent and Trademark Office to prevent the disclosure of information in patent applications, for inventions made in the United States, when the diffusion of this information is deemed "detrimental to national security." Given that AI technologies are increasingly framed as strategic assets, it is likely that AI technology patent applications are already monitored by relevant government agencies, and some secrecy orders could already have been issued. However, it is questionable how effective secrecy orders can be in controlling AI and early-stage academic hardware R&D, given the narrowness of the tool (they only apply to patent applications), the near-instant online publication of new developments in these fields, and the open publication culture of the AI research community. The role of secrecy orders in AI governance is therefore likely to be quite limited.

Prepublication Screening Procedures for Security-Sensitive Publications

In the past, the USG has introduced prepublication screening procedures for research in strategically important areas such as cryptography and biotechnology. The USG could introduce a voluntary prepublication screening procedure concerning AI which would invite researchers to submit paper drafts to a government body for review. The government body could then recommend that researchers edit or refrain from publishing any content that it deems particularly security sensitive. However, unless risks from dual-use AI research become much more immediate and severe, researcher participation levels would likely be very low. Prepublication screening is in tension with the community's culture of openness, international collaboration, and competition to publish quickly. The sheer size of the AI research community would also make the implementation of such a procedure logistically difficult, unless it was limited to highly specific subfields. The USG could also implement mandatory prepublication reviews for USG-funded research in accordance with NSDD-189, though such procedures would face similar, if not stronger, obstacles as voluntary procedures.

The Defense Production Act

The Defense Production Act (DPA) of 1950, as amended, confers upon the president a broad set of authorities to require private companies to supply products, materials, and services in the interest of the "national defense." While, at present, it is difficult to imagine why and how the USG would apply the DPA to AI, it could plausibly prioritize industry design and fabrication of AI-specific chips customized for USG needs. A government strategy could be to try to recruit top AI technology researchers into the National Defense Executive Reserve (NDER) under DPA Title VII. The NDER is a reserve of highly qualified individuals from industry to serve in civilian positions in the federal government during a national

emergency. However, the procedure for reservists to join the NDER is by application; thus, it is not possible to force top AI researchers to join the volunteer pool. Given demonstrations of anti-military sentiment among top AI researchers, voluntary participation would likely be limited unless there were sufficiently radical changes in the security landscape.

Antitrust Enforcement

Lawsuits charging harm from anticompetitive behavior or excessive market power (called "antitrust" lawsuits in the United States and "competition law" in Europe) can profoundly impact the business prospects of major tech companies: they could lead them to be broken up, charged with massive fines, or otherwise have their business constrained by strict regulations. Though the USG has not engaged in major antitrust action against a large software company since Microsoft in 2001, major tech companies are under significant scrutiny from e.g. policymakers who are actively considering updates to antitrust legislation. The USG has, on the other hand, frequently taken antitrust action against semiconductor companies. While this lever could be a powerful tool to increase the USG's access to AI technologies, it is also hard to wield for purposes other than its nominal goal. First, both tradition and law strongly constrain the government's ability to use antitrust for national security purposes. Second, even if the USG were to try to condition its nonintervention via antitrust enforcement on national security cooperation, there would be substantial legal limitations on its ability to do so. Third, it is far from clear that increased antitrust enforcement would promote national security interests.

The "Born Secret Doctrine"

Under the Atomic Energy Act of 1946, the USG introduced a pervasive system of governmental secrecy and control for all R&D information related to nuclear weapons design and testing as well as certain research on the production of nuclear power. Under the act, all information that is deemed relevant to the production of nuclear weapons, the production of special nuclear material, and the use of special nuclear material in energy production is "born classified." A similar law for certain types of AI R&D would have far-reaching consequences. The introduction of such a tool, however, is highly improbable in the current context. There is no obvious motive for the USG to introduce it at present, especially since it would be considered unconstitutional by many legal experts. Such strict limitations would also run counter to the open research culture of the AI research community. Thus, such a doctrine would likely trigger significant backlash.

Table of Contents

List of Tables

Introduction

Aims of the Report

Technology has historically been a central matter of national security interest. As such, governments have developed tools to stimulate its development and control its proliferation. During the Cold War, the United States government (USG) in particular established and used a wide variety of levers to influence the development and proliferation of strategically relevant technologies like nuclear weapons, cryptography, and, later, biotechnology. Recently, the USG has taken a strong interest in AI as a strategic technology. It has already used some of the policy levers at its disposal, such as increasing federal funding for AI R&D, screening foreign investments into AI-focused companies, and applying export controls across hardware supply chains. It has also articulated further plans to limit exports of specific AI technologies. Currently, the U.S. is the global leader in AI. Therefore, understanding the mechanisms through which the USG already influences and might influence AI R&D in the future is relevant to AI governance globally.

This report aims to provide an accessible review of some of the USG's policy levers under existing law and a preliminary analysis of how the USG could (or already does) use these levers to shape AI research, development, and deployment in pursuit of its national interests. We focus on levers that most directly support or restrict the activities of domestic non-state actors, such as AI companies, academic researchers, and nonprofit entities. This report is primarily intended for AI governance researchers. Though the report does not seek to make recommendations, it does speak to what policy levers the USG is likely to employ.

Methodology

We began the process of writing this report by compiling a list of policy levers available to the USG, based on our previous research, which could be relevant to AI and semiconductor research, development, and deployment. We then solicited ideas for additional levers from a range of experts familiar with legislation on strategically relevant technologies. However, we did not conduct a systematic search to identify all possible levers; the list we present is not exhaustive.

In our analysis of the individual levers, we relied solely on publicly available information and information provided by subject-matter experts. The inferences we draw about potential applications to AI and semiconductor R&D are necessarily somewhat subjective, but we aimed to make our reasoning as transparent as possible. Prior to publishing this report, we solicited extensive feedback from additional experts and practitioners in the field. We do not attempt a comprehensive assessment of the policy levers we mention.

Scope of Analysis

AI systems are machines capable of sophisticated information processing.[5] This includes both systems developed using machine learning (ML) techniques and systems developed by researchers working within

[5] Allan Dafoe, "AI Governance: A Research Agenda" (Oxford, UK: Governance of AI Program, Future of Humanity Institute, University of Oxford, 2018), 5, https://www.fhi.ox.ac.uk/wp-content/uploads/GovAI-Agenda.pdf.

the "symbolic" or "good old fashioned AI" (GOFAI) paradigms. We define the broader category *AI technologies* to include both AI systems and computer hardware that enables the production and use of AI systems.[6]

We focus on policy levers that are:

- *Domestic*, i.e., most directly constraining or supporting the activities of U.S.-based actors.[7]
- *Formal*, i.e., based on laws or other explicit government regulation, as opposed to informal sources of coercive or noncoercive influence.
- *Direct*, as opposed to more indirect measures such as changing incentives provided by tax or intellectual property law, for example.
- *Based on existing legislation,* though not necessarily applicable to AI or similar industries in their current form, as opposed to entirely novel influence mechanisms that might be introduced by new law.[8]

We discuss the following dimensions for each lever:

- national security objectives that might motivate the lever's use;
- the lever's legislative basis;
- the key decision-makers and implementing agencies;
- the actors most likely to be affected by the lever, e.g., multinational firms, academic researchers, and nonprofit organizations;
- the lever's origin and previous applications;
- the lever's potential application to the research, development, and deployment of AI technologies, including the likelihood of implementation;
- potential barriers and costs to applying the lever; and
- future directions of research.

Below, we provide further context for three of these dimensions: specifying USG motives, evaluating barriers and costs, and assessing the likelihood of implementation.

Specifying potential USG motives

We identified three pairs of national security objectives that could motivate the USG to use a given policy lever. Each pair consists of cultivating a national asset on the one hand and depriving a perceived rival of that asset on the other. Some levers affect progress toward a single goal; others toward multiple.

- The USG may seek to make or keep particular AI technologies and their core components available for direct use by its defense and intelligence agencies. The converse objective is to undermine the ability of a rival state's defense and intelligence agencies to use the same technology.

---

[6] These chips include graphics processing units (GPUs), field-programmable gate arrays (FPGAs), and application-specific integrated circuits (ASICs).

[7] As noted above, this excludes diplomacy, foreign intelligence collection, military operations, and other levers that most directly influence other states. It does include visa policies, foreign investment restrictions, and export controls, however, since these constrain the hiring, fundraising, and strategic decisions of U.S. firms.

[8] In particular, if there were sufficient national security concern, Congress could pass laws that significantly expand the USG's policy options, and executive wartime or crisis authority can be used to achieve much stronger levels of control. Consideration of these more extreme scenarios is beyond the scope of our analysis.

- The USG could aim to strengthen its domestic AI industries, more broadly, in order to achieve downstream economic and military benefits, or, conversely, to weaken a rival's industries.[9]
- The USG could seek to gain strategically important information about the AI technology research and development landscape, e.g., to improve foresight and provide a basis for future policy. The converse goal is to deprive a rival of this strategically important information.

Evaluating barriers and costs

Many of the policy levers in this report were created during the Cold War to manage the economic and technological competition between the U.S. and the Soviet Union. That environment is very different from the context in which AI technologies are currently being developed. These differences inform large parts of our analysis of the likely difficulty and cost of applying the levers to AI R&D. Some of the most distinct differences are:

- Cutting-edge AI R&D is primarily led by powerful technology companies as opposed to government research programs or academic research institutes. These private actors could consider legal action against the USG or could relocate to other jurisdictions, or threaten to do so, while structuring operations to avoid extraterritorial USG influence.
- The leading nations in AI—e.g., the U.S., Canada, the United Kingdom, and China—and the leading nations in semiconductors—the U.S., South Korea, Taiwan, Japan, the Netherlands, and increasingly China—have high levels of trade interdependence compared with the U.S. and the Soviet Union during the Cold War. This increases the expected costs of trade and visa restrictions due to a greater reliance on non-U.S. inputs.
- The culture of the AI research community can be characterized as "open," with new developments being disseminated quickly across organizations and borders. This is markedly different from the historical research culture in areas like nuclear physics and cryptography which, for a time, were dominated by government-led, classified research efforts. This open culture could, for example, make it harder to influence the publication of AI research.

We explore these implications in more detail in the relevant sections.

Assessing the likelihood of implementation

The levers are presented in order of our subjective assessment of their likelihood of implementation in the context of AI technologies, starting with those already in use. While we consider it unlikely that certain levers would ever be applied to AI, our aim, for completeness, is to discuss a wide range of levers that have been used by the USG in the past.

Our assessment of likelihood is informed in large part by how well each lever can be justified on national security grounds. In times of "normal" peacetime politics, many of these tools are not easily available to the USG, at least not without incurring substantial political costs. In times of perceived national security crisis, however, these tools become more available. We highlight these considerations in the report where appropriate, as they apply more strongly to some tools than others.

[9] Jeffrey Ding and Allan Dafoe, "The Logic of Strategic Assets: From Oil to Artificial Intelligence," January 9, 2020, http://arxiv.org/abs/2001.03246.

Ultimately, if there were sufficient national security concern, Congress could pass laws providing entirely novel policy levers, and executive wartime or crisis authority could be used to achieve much stronger levels of influence. Consideration of these more extreme scenarios is beyond the scope of our analysis.

AI Policy Levers

Federal R&D Funding

Potential Motives for Use	(1) Strengthen the domestic AI and semiconductor industries; (2) Make/keep relevant AI technologies available for national security purposes; (3) Gain insights into particular AI projects or the AI R&D landscape.
Legislation/Key Documents	Executive Order on Maintaining American Leadership in Artificial Intelligence, The National Artificial Intelligence Research and Development Strategic Plan 2019, Report to the President: Ensuring Long-Term U.S. Leadership in Semiconductors, Supplement to the President's FY2020 Budget.
Key Decision-Makers	National Science and Technology Council, Office of Management and Budget (among several actors who inform how federal R&D funding is allocated and spent).
Affected Actors	U.S. AI R&D actors (primarily universities, government labs).

Table 2: Federal R&D Funding Summary

Federal funding played a key role in establishing U.S. technological supremacy during the Cold War. In the 1950s, the U.S. federal government began to dominate global R&D spending, with military R&D constituting a large fraction of it. In 1960, the United States accounted for a striking 69% of global R&D, with defense-related R&D alone accounting for more than one-third of the global total. Notably, at this time, the federal government funded approximately twice as much R&D as U.S. businesses did.[10] The GPS and ARPANET, the precursor to the Internet, are two well-known outcomes of state-funded R&D projects.[11]

Since 1960, the share of federally funded R&D in the U.S. has declined relative to private R&D, from 65% to 24% in 2016.[12] U.S. R&D funding as a share of global R&D funding has also declined. In 2016, U.S. R&D funding stood at only 28% of the global total, compared to 69% in 1960. Although the U.S. maintains its leading position as the world's greatest spender on R&D with $582 billion in 2018, the relative increase by other countries is noteworthy. China's R&D spending, for example, has increased from around $33

[10] Graham R Mitchell, "The Global Context for U.S. Technology Policy." (Washington, DC: U.S. Dept. of Commerce, Office of Technology Policy, 1997), p.3, https://permanent.fdlp.gov/lps12230/nas.pdf.
[11] Thomas Heinrich (2002). Cold War Armory: Military Contracting in Silicon Valley. *Enterprise & Society*, vol.3, pp. 247–284; John A Alic et al., *Beyond Spinoff: Military and Commercial Technologies in a Changing World* (Boston, Mass.: Harvard Business School Press, 1992).
[12] John F. Sargent Jr., Marcy E Gallo, and Moshe Schwartz, "The Global Research and Development Landscape and Implications for the Department of Defense" (Washington, DC: Congressional Research Service, November 8, 2018), https://fas.org/sgp/crs/natsec/R45403.pdf.

billion in 2000 to around $554 billion in 2018, as measured in current-year purchasing power parity USD (nominal). In 2016, China's share of global R&D funding stood at 25.1%, closely behind the U.S.'s.[13]

R&D funding mechanisms differ in their levels of government involvement. The National Science Foundation (NSF) is an example of a grantmaking organization with minimal involvement. Founded in 1950 as an independent federal agency, the NSF serves "to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense…"[14] Its annual budget of around $8.1 billion (fiscal year 2019) accounts for only 4.3% of the total federal R&D budget but 14% of basic research funding.[15] The NSF mainly funds U.S. organizations and only rarely issues grants to foreign organizations. It gives most grants to researchers affiliated with colleges, universities, and academic consortia (78% of funding). Other recipients are affiliated with private industry (13%) and federally funded R&D centers (4%).[16] Its seven programmatic directorates solicit grant applications via so-called program descriptions, announcements, or solicitations. An independent assessment, conducted by a panel of domain experts and centered on the intellectual merit and broader societal impact of each application, serves as the primary basis for all funding decisions. NSF program managers have little discretion to act counter to that assessment when making the final decisions about which grants to issue.

After making a grant, "[t]he grantee has full responsibility for the conduct of the project or activity supported under an NSF grant and for the results achieved."[17] Since the 1980 Bayh-Dole Act, grantees may patent and license intellectual property from government-funded research projects. Federal agencies may only claim patent rights if the grantee and inventor waive their rights and as long as this does not limit the dissemination of the research results in the scientific community. While the NSF only supports unclassified research, growing fears of Chinese espionage have prompted changes: in 2018, the NSF restricted some program manager roles to U.S. citizens (and citizenship applicants) and, a year later, it decided to review further measures.[18]

By contrast, the Defense Advanced Research Projects Agency (DARPA) maintains a high level of influence over its funded projects. It uses its $3.4 billion budget (FY2019) to develop breakthrough technologies that enhance U.S. national security. DARPA no longer has substantial in-house research capacities. Instead, program managers at DARPA find external grantees or establish collaborative projects with academic groups or companies (both domestic and foreign) to carry out their program objectives. Program managers are expected to influence the technical direction of each project. Throughout the project lifecycle, they review preset milestones and maintain regular contact with project partners. Many of the projects and much of the project-related information are classified. Intellectual property agreements are negotiated in advance, but DARPA usually will not prevent commercialization of intellectual property that results from their projects.

---

[13] "Main Science and Technology Indicators," OECD, 2018, https://stats.oecd.org/Index.aspx?DataSetCode=MSTI_PUB#.
[14] U.S. Congress, "National Science Foundation Act of 1950" (1950), https://www.nsf.gov/about/history/legislation.pdf.
[15] John F. Sargent Jr., "Federal Research and Development (R&D) Funding: FY2020" (Congressional Research Service, March 18, 2020), https://fas.org/sgp/crs/misc/R45715.pdf.
[16] The remaining 5% are categorized as "Other." Source: National Science Foundation, "Funding and Support Descriptions," https://www.nsf.gov/homepagefundingandsupport.jsp.
[17] National Science Foundation, "Proposal & Award Policies & Procedures Guide (Chapter VII - Grant Administration)," https://www.nsf.gov/pubs/policydocs/pappg20_1/pappg_7.jsp.
[18] Jeffrey Mervis, "Elite Advisers to Help NSF Navigate Security Concerns," *Science* 363, no. 6433 (March 22, 2019): 1261–1261, https://doi.org/10.1126/science.363.6433.1261.

At the same time, it usually retains a wide-ranging "Government Purpose rights" license,[19] and resulting patents can be classified based on the Invention Secrecy Act (see this section for more details).

DARPA is only a small (~3.4% in FY2019) part of the Research, Development, Test & Evaluation (RDT&E) budget[20] of the Department of Defense (DoD). The DoD spends much more as part of its Defense Acquisition System. In collaboration with private contractors (including foreign ones[21]), this process facilitates the development and acquisition of new systems to be deployed by the armed forces. It starts with the identification of a capability gap, i.e., a difference between military needs and current capabilities. The DoD will then conduct analyses and tests to specify the systems required to meet this need. This may already include basic development activities. Based on this assessment, the DoD will issue a Request for Proposals (RFP). Typically, this is an open application process during which companies compete for the procurement contract. This can be a multistep process involving, e.g., competitive prototyping. The USG then signs a contract with the winning firm. Usually, this is followed by further development and testing until the system enters full production. All such development and testing activities prior to production are funded as part of the RDT&E budget. The DoD exerts influence over this development process by specifying capabilities, performance levels, and other requirements. These are iteratively refined throughout the acquisition process and ultimately defined in the contract between the DoD and the private firm. It then becomes the responsibility of that firm to deliver a system that fulfills these requirements. After that point, the DoD program managers typically retain less influence over the technical direction of the project compared to DARPA.

As with DARPA's programs, it is common for many aspects of DoD acquisition processes to be classified. Recently, the DoD has started to consider even more widespread classification to prevent competitors from accessing crucial information.[22] Similar to the NSF, intellectual property developed during the acquisition process is subject to the Bayh-Dole Act.[23] Under the act, the contractor can opt to patent inventions if they so choose (subject to the Invention Secrecy Act). In any case, the USG retains at least a nonexclusive, nontransferable, irrevocable, paid-up license to use the invention for government purposes. Its rights to technical data depend on the funding structure: no restrictions on disclosure and use in the case of exclusive government funding ("unlimited rights"); disclosure and use limited to within the USG in the case of exclusive private funding ("limited rights"); or disclosure and use limited to government purposes, which generally include activities for which the government is a party,[24] in case of mixed funding ("government purpose rights").

---

[19] This license allows the government to use, modify, reproduce, release, or disclose the technical data or computer software within the government without restriction and outside the government for a government purpose, including for competitive procurement, but not for commercial purposes.
[20] This budget does not include the acquisition of operational systems. It does include prototyping during the acquisition process.
[21] Larry Makinson, "Outsourcing the Pentagon," The Center for Public Integrity, September 29, 2004, https://publicintegrity.org/national-security/outsourcing-the-pentagon/.
[22] Paul McLeary, "Pentagon To Classify More Acquisition Info, Keep Closer Eye On Fed Employees," *Breaking Defense*, October 2, 2019, https://breakingdefense.com/2019/10/pentagon-to-classify-more-acquisition-info-keep-closer-eye-on-fed-employees/.
[23] See this article for further information: Gregg S. Sharp, "A Layman's Guide to Intellectual Property in Defense Contracts," *Public Contract Law Journal* 33, no. 1 (2003): 99–137, https://www.jstor.org/stable/25755261.
[24] For instance, such "government purpose rights" would even allow a government-contracted third party to use the intellectual property in the context of a procurement contract, which would not be possible under "limited rights."

Federal Funding for AI R&D

Providing funding is one possible way for the USG to shape the objectives and trajectory of AI R&D projects. There are different ways in which the U.S. could use this lever. The USG can provide funding for basic AI technology research, through organizations such as the NSF and DoD, and use its position as a sponsor to influence the objectives of these projects to varying degrees. For instance, the DoD could fund the development of specific AI systems with national security applications.[25]

Recently, the USG has increased its funding for AI R&D. The U.S. government has long relied on bottom-up, industry-guided R&D to maintain U.S. superiority in AI. However, in response to Executive Order 13859 "Maintaining American Leadership in Artificial Intelligence" and in support of The National Artificial Intelligence Research and Development Strategic Plan, AI became its own category in the president's budget request for 2020, with approximately $1 billion sought in R&D funding for nondefense purposes (67% on projects directly related to AI and 33% on projects related to adjacent areas like robotics, data science, human-machine interaction, and cybersecurity).[26] The enacted budget for FY2020 surpassed this request by about $150 million, and the president requested another increase of about $400 million for FY2021, representing a 34.4% increase over the FY2020 enacted investments.[27] Furthermore, the National Security Commission on AI recommended steep increases to federal AI R&D funding, doubling non-defense AI R&D to reach $32 billion by FY2026.[28]

Similarly, R&D investment in AI for defense purposes also increased in the last few years. According to the DoD's FY2020 budget proposal, it planned to spend $3.7 billion on "Unmanned/Autonomous projects" to "enhance freedom of maneuver and lethality in contested environments" and approximately $0.9 billion on "Artificial Intelligence / Machine Learning investments to expand military advantage through the Joint Artificial Intelligence Center (JAIC) and Advanced Image Recognition."[29] In the DoD's FY2021 budget proposal, these numbers ran to $1.7 billion and $0.8 billion respectively.[30] Strictly speaking, they also include funding not spent on R&D, but, given the early stage of the technology, a large share will likely be dedicated to R&D. While this suggests a coming decrease from FY2020 to FY2021, the overall levels have still increased notably compared to R&D investments of only around $1.8 billion in similar categories in FY2017.[31] This

---

[25] This may be difficult to achieve in the current climate among American AI companies, given that across 2018 and 2019 there were several high profile events involving AI companies such as Google facing backlash from their employees for engaging with DoD contracts. See, e.g., Samantha Maldonado, "Employees of Big Tech Are Speaking out like Never Before," *AP News*, August 25, 2019, https://apnews.com/80c76d32c7de48269cbd7bb9f838834c; Scott Shane and Daisuke Wakabayashi, "'The Business of War': Google Employees Protest Work for the Pentagon," *The New York Times*, April 4, 2018, https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html.

[26] National Science & Technology Council, "The Networking & Information Technology Research & Development Program Supplement to the President's FY2020 Budget", September 2019, https://www.whitehouse.gov/wp-content/uploads/2019/09/FY2020-NITRD-AI-RD-Budget-September-2019.pdf.

[27] The White House Office of Science and Technology Policy, "Artificial Intelligence & Quantum Information Science R&D Summary: Fiscal Years 2020-2021", August 2020, https://www.whitehouse.gov/wp-content/uploads/2017/12/Artificial-Intelligence-Quantum-Information-Science-R-D-Summary-August-2020.pdf.

[28] "Final Report" (National Security Commission on Artificial Intelligence, March 2021), 188-189, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf

[29] U.S. Department of Defense, "DOD Releases Fiscal Year 2020 Budget Proposal", March 12, 2019, https://www.defense.gov/Newsroom/Releases/Release/Article/1782623/dod-releases-fiscal-year-2020-budget-proposal/.

[30] U.S. Department of Defense, "DoD Releases Fiscal Year 2021 Budget Proposal", February 10, 2020, https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/fy2021_Press_Release.pdf.

[31] Andrew P Hunter and Lindsey R Sheppard, "Artificial Intelligence and National Security: The Importance of the AI Ecosystem" (Center for Strategic and International Studies, November 5, 2018),

signals a shift in USG thinking, pointing towards a more active role in AI R&D funding, with the Biden administration likely increasing AI funding.[32]

For hardware, U.S. industry R&D likewise overshadows USG R&D. The USG spends $1.5 billion per year on semiconductor R&D,[33] of which $300 million is from DARPA's Electronics Resurgence Initiative (ERI).[34] The ERI funds research on materials, specialized chip designs, integration of multiple specialized chip designs, and chip security.[35] Under the ERI, DARPA's Real Time Machine Learning program funds research on automated design of AI-specific ASICs.[36] Other programs focus on improving computing performance and efficiency with emerging hardware approaches beyond traditional Moore's Law–driven transistor density increases.[37] However, this USG spending pales next to the U.S. semiconductor industry's $38.7 billion R&D spending in 2018,[38] accounting for 60% of global semiconductor industry R&D spending.[39] In light of this, the National Security Commission on AI recommended a $12 billion boost in federal investment between FY2021 and FY2026.[40]

The DoD is a consumer of commercial AI-relevant chips and also maintains a Trusted Suppliers program that accredits U.S. semiconductor firms to produce custom chips for the DoD if those firms secure their manufacturing processes.[41] Currently, the U.S. lacks foundries capable of manufacturing state-of-the-art AI-relevant chips customized for national security applications.[42] To remedy this deficiency, the pending National Defense Authorization Act for Fiscal Year 2021 authorizes billions of dollars of incentives for

---

https://www.csis.org/analysis/artificial-intelligence-and-national-security-importance-ai-ecosystem. The report aggregated defense R&D spending in "Learning and Intelligence," "Advanced Computing," and "AI Systems."

[32] Sara Castellanos, "Executives Say $1 Billion for AI Research Isn't Enough," *Wall Street Journal*, September 10, 2019, https://www.wsj.com/articles/executives-say-1-billion-for-ai-research-isnt-enough-11568153863.
Sara Castellanos, "AI, Quantum R&D Funding to Remain a Priority Under Biden", *Wall Street Journal*, November 9, 2020, https://www.wsj.com/articles/ai-quantum-r-d-funding-to-remain-a-priority-under-biden-11604944800.

[33] "Winning the Future: A Blueprint for Sustained U.S. Leadership in Semiconductor Technology" (Semiconductor Industry Association, April 2019), 9, https://www.semiconductors.org/wp-content/uploads/2019/04/FINAL-SIA-Blueprint-for-web.pdf.

[34] Samuel K. Moore, "DARPA'S $1.5-Billion Remake of U.S. Electronics: Progress Report," *IEEE Spectrum*, June 27, 2019, https://spectrum.ieee.org/tech-talk/semiconductors/devices/darpas-15billion-remake-of-us-electronics-progress-report.

[35] *Id.*

[36] "Designing Chips for Real Time Machine Learning," DARPA, March 21, 2019, https://www.darpa.mil/news-events/2019-03-21.

[37] "DARPA Electronics Resurgence Initiative," DARPA, April 2, 2020, https://www.darpa.mil/work-with-us/electronics-resurgence-initiative.

[38] "2019 Factbook" (Semiconductor Industry Association, May 2019), 17, https://www.semiconductors.org/wp-content/uploads/2019/05/2019-SIA-Factbook-FINAL.pdf.

[39] Rob Lineback, "Semiconductor R&D Spending Will Step Up After Slowing," *IC Insights*, January 31, 2019, https://www.icinsights.com/news/bulletins/Semiconductor-RD-Spending-Will-Step-Up-After-Slowing/.

[40] "Final Report" (National Security Commission on Artificial Intelligence, March 2021), 218-220, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf

[41] Kristen Baldwin, "DoD Electronics Priorities" (NDIA Electronics Division, January 18, 2018), 4, https://www.ndia.org/-/media/sites/ndia/divisions/electronics/past-proceedings/ndia-ed-baldwin-18jan2018-vf.ashx?la=en. Although it was a key customer in the early days of the semiconductor industry, the DoD now accounts for less than 1% of chip purchases and has lost most of its influence over industry priorities. Khalid Alothman et al., "Spring 2017 Industry Study: Electronics" (The Dwight D. Eisenhower School for National Security and Resource Strategy, National Defense University, 2017), 17, https://es.ndu.edu/Portals/75/Documents/industry-study/reports/2017/es-is-report-electronics-2017.pdf.

[42] Mark Lapedus, "A Crisis In DoD's Trusted Foundry Program?," *Semiconductor Engineering*, October 22, 2018, https://semiengineering.com/a-crisis-in-dods-trusted-foundry-program.

reshoring advanced chip manufacturing to the United States,[43] and the USG has encouraged U.S.-based chipmaker Intel to build a state-of-the-art trusted foundry.[44] Given a push from the USG, chipmaker TSMC has announced plans to build an advanced foundry in the United States.[45] However, as TSMC is based in Taiwan, the DoD may be less likely to use TSMC's U.S. foundry than a potential Intel foundry.

[43] U.S. Congress, "S.Amdt.2244 to S.Amdt.2301 to S.4049," July 21, 2020, https://www.congress.gov/amendment/116th-congress/senate-amendment/2244/text.

[44] Asa Fitch, Kate O'Keeffe, and Bob Davis, "Trump and Chip Makers Including Intel Seek Semiconductor Self-Sufficiency," *Wall Street Journal*, May 11, 2020, https://www.wsj.com/articles/trump-and-chip-makers-including-intel-seek-semiconductor-self-sufficiency-11589103002.;
"First Quarter Recommendations" (National Security Commission on Artificial Intelligence, March 2020), 46–49, https://drive.google.com/file/d/1wkPh8Gb5drBrKBg6OhGu5oNaTEERbKss/view.;
"Final Report" (National Security Commission on Artificial Intelligence, March 2021), 212-220, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf

[45] Bob Davis, Kate O'Keeffe, and Asa Fitch, "Taiwan Firm to Build Chip Factory in U.S.," *Wall Street Journal*, May 15, 2020, https://www.wsj.com/articles/taiwan-company-to-build-advanced-semiconductor-factory-in-arizona-11589481659.

Foreign Investment Restrictions

Potential Motives for Use	(1) Undermine a rival's ability to use AI technology for national security purposes; (2) Deprive a rival of insights into particular AI projects or the AI R&D landscape.
Legislation/Key Documents	Executive Order 11858; Defense Production Act, Section 721 (Exon-Florio Amendment);The Foreign Investment & National Security Act of 2007 (FINSA); Foreign Investment Risk Review Modernization Act (FIRRMA); Export Reform Control Act of 2018 (ECRA).
Key Decision-Makers	Committee on Foreign Investment in the United States (CFIUS) chaired by the U.S. secretary of treasury (including representatives from sixteen departments and agencies); U.S. president.
Affected Actors	Select non-U.S. governments and AI and semiconductor companies (deprived of access to strategic technologies); U.S.-based AI and semiconductor companies (reduced access to capital).

Table 3: Foreign Investment Restrictions Summary

The Committee on Foreign Investment in the United States (CFIUS) is a federal interagency body with the mandate to review certain foreign investments in U.S. companies or real estate transactions on national security grounds. CFIUS can recommend to the president to block or unwind an investment. Today, the committee is chaired by the secretary of the treasury and includes representatives from sixteen U.S. departments and agencies including the Department of Defense, Department of State, Department of Commerce, and Department of Homeland Security.[46]

CFIUS was initially created in 1975 by President Gerald Ford through Executive Order 11858 in response to surging investment from oil-producing countries.[47] The executive order stipulated that the committee would have "primary continuing responsibility within the Executive Branch for monitoring the impact of foreign investment in the United States, both direct and portfolio, and for coordinating the implementation of United States policy on such investment."[48] In 1988, Section 721 of the Defense Production Act (the so-called Exon-Florio Amendment) was enacted, which gives the president the authority to block an acquisition when there is "credible evidence" that a "foreign interest exercising control might take action that threatens to impair national security."[49] The Exon-Florio Amendment resulted from U.S. national security concerns regarding the proposed takeover of Fairchild Semiconductor by the Japanese company

[46] U.S. Department of the Treasury, "The Committee on Foreign Investment in the United States (CFIUS)," 2021, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius.
[47] Matthew P. Goodman and David A. Parker, "The China Challenge and CFIUS Reform," *CSIS Global Economics Monthly*, March 31, 2017, https://www.csis.org/analysis/global-economics-monthly-china-challenge-and-cfius-reform.
[48] The White House, "Executive Order 11858--Foreign Investment in the United States," May 7, 1975, https://www.archives.gov/federal-register/codification/executive-order/11858.html.
[49] James K Jackson, "The Committee on Foreign Investment in the United States (CFIUS)" (Congressional Research Service, February 14, 2020), 7, https://fas.org/sgp/crs/natsec/RL33388.pdf.

Fujitsu. In 2007, the existing CFIUS practice was enshrined in the Foreign Investment and National Security Act (FINSA).[50]

Foreign Investment Restrictions and AI R&D

CFIUS has already been used and adapted with specific reference to AI and semiconductors. In recent years, based on CFIUS recommendations, the president blocked several Chinese attempts to buy U.S. chip makers.[51] In December 2016, then President Barack Obama blocked the Chinese acquisition of U.S. shares in the German-based company Aixtron, which produces semiconductor manufacturing equipment, on national security grounds.[52] Other notable semiconductor-related actions include President Trump, on recommendation of CFIUS, blocking Singapore-based chip design firm Broadcom from acquiring U.S.-based chip design firm Qualcomm,[53] a Chinese investment fund Hubei Xinyan from acquiring U.S.-based semiconductor manufacturing equipment maker Xcerra,[54] and Chinese-based Tsinghua Unigroup from acquiring Lattice Semiconductor, a U.S.-based field-programmable gate array (FPGA) maker.[55]

In 2016, the Defense Innovation Unit Experimental (DIUx) (now simply known as the Defense Innovation Unit), compiled a report entitled "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation." The authors, Michael Brown and Pavneet Singh, voiced concerns that China is circumventing CFIUS through joint ventures, minority stakes, and early-stage investments in U.S. startups to gain access to critical dual-use technologies including artificial intelligence, robotics, and semiconductors.[56]

In June 2017, with eyes on emerging technologies including AI and especially Chinese investments in these industries, Senator John Cornyn (R-Texas) announced his intention to introduce a bill to reform the

---

[50] See for example, Patrick Griffin, "CFIUS in the Age of Chinese Investment," *Fordham Law Review* 85, no. 4 (2017): 1757–92, https://ir.lawnet.fordham.edu/flr/vol85/iss4/9. Also see C. S. Eliot Kang, "U.S. Politics and Greater Regulation of Inward Foreign Direct Investment," *International Organization* 51, no. 2 (1997): 301–33, https://doi.org/10.1162/002081897550375.

[51] Muhammad Irfan, "US May Block Chinese Investment in Artificial Intelligence in Silicon Valley," *Daily Pakistan Global*, June 14, 2017, https://en.dailypakistan.com.pk/technology/us-may-block-chinese-investment-in-artificial-intelligence-in-silicon-valley/.

[52] Paul Mozur, "Obama Moves to Block Chinese Acquisition of a German Chip Maker," *The New York Times*, December 2, 2016, https://www.nytimes.com/2016/12/02/business/dealbook/china-aixtron-obama-cfius.html.

[53] David McLaughlin, "Trump Blocks Broadcom Takeover of Qualcomm on Security Risks," *Bloomberg*, March 12, 2018, https://www.bloomberg.com/news/articles/2018-03-12/trump-issues-order-to-block-broadcom-s-takeover-of-qualcomm-jeoszwnt.

[54] Greg Roumeliotis, "U.S. Blocks Chip Equipment Maker Xcerra's Sale to Chinese State Fund," *Reuters*, February 23, 2018, https://www.reuters.com/article/us-xcerra-m-a-hubeixinyan-idUSKCN1G703H.

[55] Seth Fiegerman and Jackie Wattles, "Trump Stops China-Backed Takeover of U.S. Chip Maker," *CNN Money*, September 14, 2017, https://money.cnn.com/2017/09/13/technology/business/trump-lattice-china/index.html.

[56] See Michael Brown and Pavneet Singh, "How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation" (Defense Innovation Unit Experimental, 2018), https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf. Also see Paul Mozur and Jane Perlez, "China Bets on Sensitive U.S. Start-Ups, Worrying the Pentagon," *The New York Times*, March 22, 2017, https://www.nytimes.com/2017/03/22/technology/china-defense-start-ups.html.

authority and operation of CFIUS, citing the DIUx report.[57] The bill, the so-called Foreign Investment Risk Review Modernization Act (FIRRMA), represents the most substantial reform of the CFIUS process since its inception. Through FIRRMA, Congress seeks to modernize the CFIUS process to reflect both emerging national security concerns and the increasingly complex ways that foreign businesses as well as governments invest in the United States.

Written into law in August 2018, FIRRMA significantly broadens CFIUS's jurisdiction. Before FIRRMA, only foreign investments that could result in control of a U.S. business were subject to CFIUS review. The final FIRRMA regulations that took effect in February 2020 include, among other changes, a new category of foreign investments covered by CFIUS, namely "any direct or indirect, non-controlling foreign investment in a U.S. business producing or developing critical technology, owning or operating critical infrastructure assets or maintaining or collecting sensitive personal data of U.S. citizens." Businesses falling under this category are referred to as a "TID U.S. Business." In order for a minority investment in a TID business to fall under CFIUS purview, it must meet additional criteria and provide a foreign investor with one of the following: (1) the ability to access any material nonpublic technical information in the possession of the TID U.S. Business; (2) the right to nominate a member or observer to the board of directors of the TID U.S. Business; or (3) any involvement, other than through voting of shares, in the substantive decision-making of the TID U.S. business.[58]

Critical technologies are defined through cross-references to various export controls regimes.[59] "Critical technologies" include (1) military technology and services subject to the International Traffic in Arms Regulations, (2) dual-use (civilian/military) technologies that are controlled by the Export Administration Regulations (EAR), and (3) emerging and foundational technologies under the Export Control Reform Act (ECRA) of 2018.[60] This last category—"emerging" and "foundational" technologies—is currently being established by a rulemaking proceeding of the Commerce Department where AI and semiconductors have been widely discussed (see next section on export controls).[61] Thus, the outcome of this ongoing process is important to better understand how FIRRMA will likely be applied with regard to AI and semiconductors in the future.

While it is too early to analyze the effects of FIRRMA conclusively, it is not clear that the benefits will outweigh the costs from the perspective of the USG in the longer term. While FIRRMA might help to

---

[57] Patrick Tucker, "What's the 'Risk' in China's Investments in US Artificial Intelligence? New Bill Aims to Find Out," *Defense One*, June 22, 2017, https://www.defenseone.com/technology/2017/06/how-not-win-ai-arms-race-china/138919/.

[58] John M. Beahn, Robert S. Larussa, and Lisa Raisner, "Final CFIUS Regulations Implement Significant Changes by Broadening Jurisdiction and Updating Scope of Reviews," Shearman & Sterling, January 14, 2020, https://www.shearman.com/perspectives/2020/01/final-cfius-regulations-implement-changes-by-broadening-jurisdiction-and-updating-scope-of-reviews.

[59] A company dealing with critical technologies qualifies as a "TID U.S. Business" "if it produces, designs, tests, manufactures, fabricates or develops one or more such technologies." See Dentons, "New CFIUS Rules under FIRRMA: What Foreign Investors and US Businesses Need to Know," January 24, 2020, https://www.dentons.com/en/insights/alerts/2020/january/24/new-cfius-rules-under-firrma-what-foreign-investors-and-us-businesses-need-to-know.

[60] Jonathan Gafni, Thomas A McGrath, and January Kim, "Mandatory CFIUS Filings Under the Final FIRRMA Regulations | Insights | Linklaters," Linklaters, January 28, 2020, https://www.linklaters.com/en/insights/publications/us-publications/2020/january/mandatory-cfius-filings-under-the-final-firrma-regulations.

[61] Ivan A. Schlager et al., "CFIUS Goes Back to the Future by Tying Mandatory Filings Pertaining to Critical Technologies to U.S. Export Controls Assessments," Kirkland & Ellis, October 21, 2020, https://www.kirkland.com/publications/kirkland-alert/2020/10/cfius-critical-technologies.

prevent the transfer of semiconductor technologies and early-stage developments in AI to some extent, the lever only targets a very specific channel of technology transfer. Moreover, the protection of the domestic industry using this lever comes likely at the cost of decreased investment in that industry.[62] Currently, there does not seem to be a structured approach on the side of the USG to absorb these losses for the U.S. high-tech ecosystem.

[62] See for example Heather Somerville, "Chinese Tech Investors Flee Silicon Valley as Trump Tightens Scrutiny," *Reuters*, January 7, 2019, https://www.reuters.com/article/us-venture-china-regulation-insight-idUSKCN1P10CB.

Export Controls

Potential Motives for Use	(1) Undermine a rival's ability to use AI technologies for national security purposes; (2) Weaken the rival's AI and semiconductor industries.
Legislation/Key Documents	Export Control Reform Act of 2018 (ECRA); Export Administration Regulations (EAR); Commerce Control List (CCL); International Traffic in Arms Regulations (ITAR); US Munitions List (USML)
Key Decision-Makers	U.S. president; U.S. Trade Representative, Department of State, Department of Commerce (Bureau of Industry and Security); Department of Defense (Defense Technology Security Administration); Department of Energy; Department of the Treasury (Office of Foreign Assets Control); Member States of the Wassenaar Arrangement.
Affected Actors	Select non-U.S. individuals, companies, and states (deprived of critical imports); U.S.-based AI and semiconductor companies (deprived of export opportunities); U.S.-based foreign national AI researchers and semiconductor engineers (movement and activity restrictions under "deemed exports" rule).

Table 4: Export Controls Summary

Export controls are tools to restrict the unlicensed export of objects and knowledge in pursuit of national security goals or trade protection. They are a dynamic instrument that can be adapted to changes in the security situation of a particular country. The origins of the U.S. export control system can be traced back to the time of the American Revolution, when the U.S. outlawed the export of goods to Great Britain in 1775. During the Cold War, as part of the U.S. containment strategy, the USG imposed licensing requirements on exports to Soviet Bloc countries, which resulted in the enactment of the Export Control Act of 1949—the first U.S. peacetime export control law that recognized the need for an export control system in response to a new security threat.[63]

Today, the U.S. export control system governs the export of tangible items, software, technical data, and, in some instances, services. These are covered by three different instruments: (1) the Export Administration Regulations (EAR),[64] (2) the International Traffic in Arms Regulations (ITAR),[65] and (3) the Foreign Assets

[63] Silverstone, Paul H., "The Export Control Act of 1949: Extraterritorial Enforcement," *University of Pennsylvania Law Review* Vol. 107 (1959), p. 4 & 6, https://scholarship.law.upenn.edu/cgi/viewcontent.cgi.

[64] The EAR serves to control the export of both commodities which have military and commercial applications (dual-use items). The Department of Commerce (DoC) administers the EAR through the Bureau of Industry and Security (BIS). Dual-use items subject to the EAR are identified in the Commerce Control List (CCL). See Appendix C for more details.

[65] The ITAR controls the export of defense articles, defense services, and related technical data from the United States to foreign destinations and persons. Restricted items are listed on the US Munitions List (USML). The ITAR serves to control strictly military items. The U.S. Department of State, Directorate of Defense Trade Controls (DDTC) is responsible for interpreting and enforcing the International Traffic in Arms Regulations (ITAR).

Control Regulations (FACR). U.S. export controls have historically focused on the physical export of goods. However, over time, the regulations have been expanded. Today, they also cover "intangible technology transfer" (ITT) and "deemed exports," which regulate the transfer of technical data, including software, to foreign nationals in the U.S., and "deemed reexports," meaning the release of licensed items and data with a U.S. origin to a third-country national overseas.[66] The U.S. is also part of several multilateral export control regimes including the Wassenaar Arrangement, which promotes transparency and responsibility in transfers of conventional arms and dual-use goods and technologies. Through their national policies and information sharing, the participating states seek to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine regional and international security and stability.[67]

Export Controls and AI R&D

Currently, AI is to some extent covered by U.S. export control regulations.[68] Additionally, export controls are widely applied across the semiconductor supply chain, including to several types of input materials, semiconductor manufacturing equipment, and chips.[69] Notably, among AI-relevant chips, the U.S. applies the strictest controls to field-programmable gate arrays,[70] moderately controls CPUs, but only minimally controls GPUs.[71] Controls on application-specific integrated circuits specialized for AI (AI ASICs) are less clear.[72] The U.S. has also placed several entities on an export blacklist called the Entity List. Many of these entities—such as Huawei, China's National Supercomputing Centers, and Chinese AI companies aiding government surveillance of Uyghurs in China's Xinjiang province—consumed U.S.-origin AI or

---

[66] The release of controlled technology and technical data to foreign persons in the U.S. is considered as an export to the person's country or countries of nationality. Under the EAR, the export of technology or software is defined to include "any release of technology or software subject to the EAR in a foreign country; or any release of technology or source code subject to a foreign national, which is deemed to be an export to the home country or countries of the foreign national."

[67] The Wassenaar Arrangement, "About Us," 2020, https://www.wassenaar.org/about-us/.

[68] For example, 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." 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. Source: Carrick Flynn, "Recommendations on Export Controls for Artificial Intelligence" (Center for Security and Emerging Technology, February 2020), https://cset.georgetown.edu/wp-content/uploads/Recommendations-on-Export-Controls-for-Artificial-Intelligence.pdf.

[69] Category 3 of the Commerce Control List is largely directed to semiconductors. "Commerce Control List: Category 3 - Electronics" (Bureau of Industry and Security, May 23, 2019), https://www.bis.doc.gov/index.php/documents/regulations-docs/2334-ccl3-8/file. For a summary of semiconductor export controls in the Wassenaar Arrangement, which the Commerce Control List replicates, see "Measuring Distortions in International Markets: The Semiconductor Value Chain," OECD Trade Policy Papers (OECD, December 12, 2019), 39, https://www.oecd-ilibrary.org/trade/measuring-distortions-in-international-markets_8fe4491d-en.

[70] Field-programmable gate arrays (FPGAs) are a type of integrated circuits. FPGAs are controlled under ECCN 3A001.7 and technical data for FPGAs are controlled under ECCN 3E001. See "Commerce Control List: Category 3 - Electronics."

[71] For example, CPUs are controlled under ECCN 3A991 for anti-terrorism reasons and technical data for CPUs are controlled under ECCN 3E002. Id.

[72] Roszel C. Thomsen II, "Artificial Intelligence and Export Controls: Conceivable, but Counterproductive?," *Journal of Internet Law* 12, no. 5 (November 2018), 16, https://t-b.com/wp-content/uploads/2019/01/AI-and-Export-Controls-Journal-of-Internet-Law-Article.pdf. Although the Commerce Control List includes "neural network integrated circuits" and "neural computers," it is unclear which AI-specific ASICs these categories cover. Id.

semiconductor technologies.[73] The U.S. also controls exports to China's leading chipmaker, Semiconductor Manufacturing International Corporation (SMIC)—a major consumer of U.S. semiconductor manufacturing equipment—on grounds that it supports the Chinese military.[74] The USG may consider expanding existing export controls to gain leverage over the dissemination of a broader set of AI and semiconductor technologies to foreign countries, and existing "deemed exports" to decrease foreigners' access to AI and semiconductor R&D programs in university laboratories or companies in the U.S.

One indication that such a development may be on the horizon is that in November 2018 the Commerce Department issued an advance notice of proposed rulemaking (ANPRM) under the EAR to seek public input on how it should identify "emerging technologies" that are critical to U.S. national security. The notice identifies 14 technology categories that the Commerce Department regards as pertinent. It asked for comment on the status of these technologies' development in the U.S. and abroad, as well as the impact export controls would have on U.S. technological leadership.

The technology categories in the ANPRM cover a range of advanced computing, manufacturing, and sensing technologies. However, the most extensive section is dedicated to AI and ML technologies. Those currently under review include (i) neural networks and deep learning (e.g., brain modeling, time series prediction, classification); (ii) evolutionary and genetic computation (e.g., genetic algorithms, genetic programming); (iii) reinforcement learning; (iv) computer vision (e.g., object recognition, image understanding); (v) expert systems (e.g., decision support systems, teaching systems); (vi) speech and audio processing (e.g., speech recognition and production); (vii) natural language processing (e.g., machine translation); (viii) planning (e.g., scheduling, game playing); (ix) audio and video manipulation technologies (e.g., voice cloning, deep-fakes); (x) AI cloud technologies; and (xi) AI chipsets. The ANPRM also covers microprocessor technology such as systems on a chip (SoC) and stacked memory on a chip, advanced computing technology such as memory-centric logic, and quantum computing.[75]

By the end of the commenting period (January 10, 2019), the Bureau of Industry and Security (BIS) had received 245 comments, of which 231 were made public on their website.[76] Many researchers and companies criticized the proposed export controls, arguing that they would further impede the free exchange of information and ideas, create further barriers to the recruitment of skilled professionals, and place American companies at a competitive disadvantage.[77] While the National Security Commission on AI calls for increased export controls on AI technologies, it acknowledges that "present policymakers with a difficult choice between under-protection, which will give competitors unacceptable levels of access to sensitive

---

[73] "Entity List," Bureau of Industry and Security, 2019, https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list.

[74] Dan Strumpf, "U.S. Sets Export Controls on China's Top Chip Maker," *Wall Street Journal*, September 28, 2020, https://www.wsj.com/articles/u-s-sets-export-controls-on-chinas-top-chip-maker-11601118353.

[75] Bureau of Industry and Security, "Review of Controls for Certain Emerging Technologies," *Federal Register*, November 19, 2018, 58201–2, https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies.

[76] Some major AI firms including Google, Facebook, and OpenAI submitted comments on the proposed export controls. See: "OpenAI Response Regarding ANPRM Controls for Certain Emerging Technologies" (OpenAI, January 10, 2019), https://www.regulations.gov/document?D=BIS-2018-0024-0195.; "Facebook Inc. ANPRM Comments" (Facebook, January 10, 2019), https://www.regulations.gov/document?D=BIS-2018-0024-0212.; "Google Comment - ANPRM - Review of Controls for Certain Emerging Technologies" (Google, January 10, 2019), https://www.regulations.gov/document?D=BIS-2018-0024-0160.

[77] Similar concerns were raised by cryptography firms and researchers in relation to proposed export controls on cryptographic technologies in the 1990s (see Appendix A for further details). Other comments raised the potential adverse effects that far-reaching export controls could have by weakening the U.S. industrial base in the long run.

technologies, and over-protection, which has the potential to stifle innovation and harm overall U.S. competitiveness."[78]

While there is no final decision on the updated export controls yet, Lynne Parker, the Deputy Chief Technology Officer of the United States at the White House Office of Science and Technology Policy, has already mentioned at an event at the Center for a New American Security in February 2019 that the list of technologies that will eventually be targeted by new export controls will be much shorter than the ANPRM suggested.[79] The Commerce Department has only begun to release new export controls on emerging technologies in 2020 after long delays. In early 2020, the Commerce Department announced new export controls targeting AI technology, specifically geospatial imagery software, under the EAR.[80] In June 2020, BIS added the first emerging technologies (certain chemical weapons precursors and biological equipment) to the Commerce Control List (CCL) in consultation with the Australia Group. In a second round, BIS added six additional emerging technologies to the CCL after these controls were agreed upon by states participating in the Wassenaar Arrangement in late 2019.[81] What is notable is that BIS has prioritized to coordinate the new controls with international partners except for the controls of geospatial imagery software. It remains to be seen whether and if so when BIS will impose additional export controls on AI and semiconductors.

In mid 2020, the Commerce Department issued a new ANPRM to define and identify "foundational technologies" for potential export controls, and specifically called out semiconductor manufacturing equipment as a candidate category.[82] The outcome of both processes will be crucial not only for future U.S. export controls regarding AI and semiconductors, but also for the application of FIRRMA.

---

[78] "Final Report" (National Security Commission on Artificial Intelligence, March 2021), 228, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf

[79] Kiran Stacey, "US Pledges to Limit Export Controls on Advanced Tech," *Financial Times*, February 28, 2019, https://www.ft.com/content/ab4313dc-3b7d-11e9-b72b-2c7f526ca5d0.

[80] Note that this was not under the ANPRM process. Source: Alexandra Alper, "U.S. Government Limits Exports of Artificial Intelligence Software," *Reuters*, January 3, 2020, https://www.reuters.com/article/usa-artificial-intelligence-idUSL1N2980M0.

[81] These six emerging technologies include hybrid additive manufacturing and computer numerically controlled tools, certain computational lithography software designed for the fabrication of extreme ultraviolet masks, technology for finishing wafers for 5nm production, forensics tools that circumvent authentication or authorization controls on a computer or communications device and extract raw data, software for monitoring and analysis of communications and metadata acquired from a telecommunications service provider via a handover interface and suborbital aircraft. See Gibson Dunn, "New Controls on Emerging Technologies Released, While U.S. Commerce Department Comes Under Fire for Delay", October 27, 2020. https://www.gibsondunn.com/new-controls-on-emerging-technologies-released-while-us-commerce-department-comes-under-fire-for-delay/#_ftn1

[82] Bureau of Industry and Security, "Review of Controls for Certain Emerging Technologies," *Federal Register* 83, no. 223 (November 19, 2018): 58201–2, https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies.

Visa Vetting

Potential Motives for Use	(1) Deprive a rival of insights into particular AI projects or the AI R&D landscape; (2) Undermine a rival's ability to use AI technologies for national security purposes.
Legislation/Key Documents	Immigration and Nationality Act (INA), 212(a)(3)(A)(i)(II); Proclamation 100043 of May 29, 2020.
Key Decision-Makers	Department of Homeland Security; State Department.
Affected Actors	Non-U.S. AI R&D actors (deprived of access to information); U.S. AI R&D institutions (deprived of access to foreign AI talent).

Table 5: Visa Vetting Summary

Visa vetting requires that visas are granted only after the applicant has been checked against certain preset criteria. In response to concerns over the illegal transfer of sensitive technologies, a process evolved during the Cold War to screen suspect visa cases, primarily from the Warsaw Pact countries, China, and Vietnam.[83] In 1998, the USG developed the Visas Mantis program due to law enforcement and intelligence community concerns that U.S.-produced goods and information are vulnerable to theft by foreign states, nationals, and companies. Suspect cases must now be flagged using the so-called Visas Mantis indicator, a preliminary pre-issuance name-check procedure used by the Department of State for visa applications. The Visas Mantis program has several objectives, including "to prevent the transfer of arms and sensitive dual-use items to terrorist states and to maintain U.S. advantages in certain military critical technologies."[84]

As part of the procedure, the consular officers use the Technology Alert List (TAL) as a guidance tool to decide whether to deny visas to particular applicants under the Immigration and Nationality Act 212(a)(3)(A)(i)(II)[85] and thereby control the potential disclosure of certain technologies to foreign persons. The TAL has two parts: Part A contains the "Critical Fields List," including, for example,[86] (i) information security: technologies associated with cryptography to ensure secrecy for communications, video data, and related software; (ii) robotics: artificial intelligence, automation, machine tools, pattern recognition

[83]At that time, the screening procedures were known as SPLEX (Soviet applicants), CHINEX (Chinese), and VIETEX (Vietnamese). See Charles Gordon, Stanley Mailman, Stephen Yale-Loehr & Ronald Y. Wada (2020). *Immigration Law and Procedure: USCIS Policy Manual & USCIS Field Adjudicator Manual.* Volume 1, Lexis Nexis.

[84] Charles Gordon, Stanley Mailman, Stephen Yale-Loehr & Ronald Y. Wada (2020). Immigration Law and Procedure: USCIS Policy Manual & USCIS Field Adjudicator Manual. Volume 1, Lexis Nexis.

[85] General classes of aliens ineligible to receive visas and ineligible for admission, waivers of inadmissibility: Sec. 212. (a) Classes of Aliens Ineligible for Visas or Admission. -Except as otherwise provided in this Act, aliens who are inadmissible under the following paragraphs are ineligible to receive visas and ineligible to be admitted to the United States (3) Security and related grounds (A) In general.-Any alien who a consular officer or the Attorney General knows, or has reasonable ground to believe, seeks to enter the United States to engage solely, principally, or incidentally in (i) any activity (II) to violate or evade any law prohibiting the export from the United States of goods, technology, or sensitive information.
U.S. Congress, "Immigration and Nationality Act," 1182 8 USC § 212, https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title8-section1182&num=0&edition=prelim.

[86] The actual TAL is classified. An old version has been leaked online: "Technology Alert List" (U.S. Department of State, August 2002), https://www.bu.edu/isso/files/pdf/tal.pdf.

technologies; and (iii) advanced computer/microelectronic technology: supercomputing, hybrid computing, speech processing, neural networks, data fusion, etc. Part B contains a list of countries that the USG deems as needing additional attention for "political, foreign policy or security reasons."[87]

Consular officers are alerted to visa applications of foreigners who are coming to the U.S. to engage in an activity involving one of the scientific fields listed in Part A of the TAL. Such activities include undergoing graduate-level studies, teaching, conducting research, participating in exchange programs, receiving training or employment, or engaging in commercial transactions. The officers can deny visas to any foreign applicant, if they have reasonable grounds to believe that the applicant is seeking entry "to engage solely, principally or incidentally in any activity to violate or evade any law prohibiting the export from the U.S. of goods, technology or sensitive information."[88] Students, scholars, and workers from the five "state sponsors of terrorism" (Cuba, Iran, North Korea, Sudan, and Syria) and the five "nonproliferation export control countries" (China, India, Israel, Pakistan, and Russia) are especially likely to be impacted. According to Kearney and Carlyle, "the visa officer's belief that an unlawful technology transfer will occur is sufficient to deny the visa."[89] There is no public record of how often the TAL is used as a basis to deny visa applications.

Additional authorities to specifically block Chinese citizens' access to visas for research or postgraduate study were granted to the State Department in a May 2020 executive order by former President Trump. According to the executive order, visa issuance will be suspended or limited for applicants with connections to any entity in China "that implements or supports the [China]'s 'military-civil fusion strategy.'"[90]

Visa Vetting and AI R&D

The USG could expand the vetting of visas to applicants in the AI and semiconductor fields, particularly to those from China. Trump's May 2020 executive order is one such example, but increased delays and denials of visa applications have been reported since 2019.[91] Such a procedure might be effective in preventing some cases of espionage and technology transfer. It may be particularly effective in minimizing the transfer of tacit knowledge, which is important to AI and unusually critical to the semiconductor industry.[92] Tacit knowledge is knowledge that is difficult to communicate explicitly in, say, a textbook, and is usually acquired through extended training and practice.[93] The importance of tacit knowledge in the AI and semiconductor industries is partly reflected in the rising competition for AI talent between the USG, private companies, and

---

[87] Julie Farnam, *US Immigration Laws under the Threat of Terrorism* (Algora Publishing, 2005), 88.
[88] Immigration and Nationality Act, 212(a)(3)(A)(i)(II) (see footnote 82).
[89] James K. Kearney and Womble Carlyle, "Export Control Regulations and Participation by Foreign Nationals in University Research" (Washington, DC, 2004), p.25, https://doi.org/10.4135/9781412969024.n90.
[90] The White House, "Proclamation on the Suspension of Entry as Nonimmigrants of Certain Students and Researchers from the People's Republic of China" May 29, 2020, https://web.archive.org/web/20210116212117/https://www.whitehouse.gov/presidential-actions/proclamation-suspension-entry-nonimmigrants-certain-students-researchers-peoples-republic-china/.
[91] Emily Feng, "Visas Are The Newest Weapon In U.S.-China Rivalry," *NPR*, April 25, 2019, https://www.npr.org/2019/04/25/716032871/visas-are-the-newest-weapon-in-u-s-china-rivalry.
[92] Taiwan relied on PhDs from U.S. universities to build its semiconductor industry. Clair Brown and Greg Linden, *Chips and Change: How Crisis Reshapes the Semiconductor Industry* (Cambridge: MIT Press, 2011), 125. Later, China attracted over 3,000 semiconductor engineers from Taiwan to build its semiconductor industry. Qiu Liling, "中國企業開出2至3倍薪資挖角 台灣已流失3000多名半導體業人才," *CMMedia*, December 3, 2019, https://www.cmmedia.com.tw/home/articles/18815.
[93] Jeremy Fantl, "Knowledge How," in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, (Metaphysics Research Lab, Stanford University, 2017), https://plato.stanford.edu/archives/fall2017/entries/knowledge-how/.

universities,[94] and the U.S. semiconductor industry's reported difficulty filling open technical positions.[95] However, it should be noted, most large-scale transfers of data and intellectual property occur not via individuals, but via cyber breaches or private investments and acquisitions.[96]

On the other hand, as outlined in the next section, a reduction in the number of visas awarded to students and skilled workers could also threaten the U.S. competitiveness in the fields of AI and semiconductors; U.S. companies currently rely heavily on foreign talent to fill widening skill gaps.[97] Enhanced vetting will make the visa application process slower and more unpredictable, which will likely make it less attractive for foreigners to study or seek employment in the U.S.

---

[94] See Jon Harper, "Pentagon Struggling to Attract Artificial Intelligence Experts," *National Defense*, July 14, 2017, https://www.nationaldefensemagazine.org/articles/2017/7/14/pentagon-in-artificial-intelligence-arms-race-with-commercial-industry.; Markoff John and Rosenberg Matthew, "China Gains on the U.S. in the Artificial Intelligence Arms Race," *New York Times (China Edition)*, February 4, 2017, https://cn.nytimes.com/world/20170204/artificial-intelligence-china-united-states/en-us/.; and Mary L. Cummings, "Artificial Intelligence and the Future of Warfare" (Chatham House, January 2017), https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings.pdf.

[95] "SIA Workforce Roundtable Summary Report" (Semiconductor Industry Association, March 16, 2018), 3, https://www.semiconductors.org/wp-content/uploads/2018/06/Roundtable_Summary_Report_-_FINAL.pdf.
Will Hunt and Remco Zwetsloot, "The Chipmakers: U.S. Strengths and Priorities in the High-End Semiconductor Workforce" (Center for Security and Emerging Technology, 2020). https://cset.georgetown.edu/research/the-chipmakers-u-s-strengths-and-priorities-for-the-high-end-semiconductor-workforce/.

[96] Remco Zwetsloot et al., "Keeping Top AI Talent in the United States" (Center for Security and Emerging Technology, December 2019), https://cset.georgetown.edu/wp-content/uploads/Keeping-Top-AI-Talent-in-the-United-States.pdf.

[97] Remco Zwetsloot, Roxanne Heston, and Zachary Arnold, "Strengthening the U.S. AI Workforce" (Center for Security and Emerging Technology, September 2019), https://cset.georgetown.edu/wp-content/uploads/CSET_U.S._AI_Workforce.pdf.
Will Hunt and Remco Zwetsloot, "The Chipmakers: U.S. Strengths and Priorities in the High-End Semiconductor Workforce" (Center for Security and Emerging Technology, 2020). https://cset.georgetown.edu/research/the-chipmakers-u-s-strengths-and-priorities-for-the-high-end-semiconductor-workforce/.
"SIA Workforce Roundtable Summary Report" (Semiconductor Industry Association, March 16, 2018), 3, https://www.semiconductors.org/wp-content/uploads/2018/06/Roundtable_Summary_Report_-_FINAL.pdf.
Remco Zwetsloot et al., "The Immigration Preferences of Top AI Researchers: New Survey Evidence" (Perry World House and The Future of Humanity Institute, 2021), https://global.upenn.edu/perryworldhouse/news/immigration-preferences-top-ai-researchers-new-survey-evidence.

Expanded Visa Pathways

Potential Motives for Use	(1) Strengthen domestic AI and semiconductor industries; (2) Weaken a rival's AI and semiconductor industries.
Legislation/Key Documents	Immigration and Nationality Act (INA).
Key Decision-Makers	Department of Homeland Security; State Department.
Affected Actors	U.S.-based AI R&D institutions (increased access to foreign talent); non-U.S. AI R&D institutions (reduced access to talent).

Table 6: Expanded Visa Pathways Summary

Immigration can be restricted for reasons of national security, but it can also be expanded to secure key talent for strategic industries while preventing competitors from recruiting the same people. Operation Paperclip is one famous example of such an effort.[98] Between 1945 and 1990, around 1,600 German scientists, engineers, and technicians were brought into the U.S. to be employed in important strategic industries, e.g., aeronautics and rocketry, chemical engineering, and electronics. Toward the end of the Second World War, military and civilian experts started surveying the state of German technological development and came to believe that in many areas it was superior to the U.S.'s. At the same time, USG officials and industry leaders saw increasing evidence that the British, French, and Russians sought to recruit the Germans who had been responsible for these advances. To counter these efforts and further U.S. national security and economic competitiveness, they appealed to President Truman to facilitate the entry and employment of top German scientists and engineers. After bureaucratic infighting and delays, President Truman approved the Paperclip directive on September 3, 1946. It facilitated the entry of up to 1,000 selected Germans and Austrians under military custody until their eligibility for visas, permanent residency, and eventual citizenship had been determined. The program continued in different forms until 1990.

Operation Paperclip was clearly a product of its time, and is likely far more radical than measures currently being considered by the USG. Nevertheless, it provides a historical example of a measure put in place to recruit top foreign talent for critical industries.

Expanded Visa Pathways and AI R&D

While there is no strong evidence that the USG is actively considering expanded visa pathway options for the AI field in the near future, the Center for Security and Emerging Technology, a Washington, DC, based think tank, has outlined several options in this vein for foreign AI and semiconductor researchers and workers.[99] First, the USG could increase the current caps on green cards and H-1B visas or selectively lift

[98] Linda Hunt, *Secret Agenda: The United States Government, Nazi Scientists, and Project Paperclip, 1945 to 1990* (New York: St. Martin's Press, 1991).
John Gimbel, "Project Paperclip: German Scientists, American Policy, and the Cold War," *Diplomatic History* 14, no. 3 (1990): 343–65, https://www.jstor.org/stable/24911848.

[99] You can find more information about different immigration reform options in three reports by the Center for Security & Emerging Technology:

- Zachary Arnold et al., "Immigration Policy and the U.S. AI Sector" (Center for Security and Emerging Technology, September 2019), https://cset.georgetown.edu/wp-content/uploads/CSET_Immigration_Policy_and_AI.pdf.

them for AI and semiconductor professionals. Second, the USG could update criteria for granting O-1 temporary visas and EB-1 green cards to better cover AI and semiconductor workers[100]. Third, it could codify the Optional Practical Training program for recent university graduates who obtained an AI- or semiconductor-relevant degree. Fourth, it could introduce a visa program for workers committing to government service in AI-related projects, similar to the Military Accessions Vital to National Security (MAVNI) program of the Department of Defense. Fifth, it could eliminate obstacles and backlogs in the visa application process as well as improve the flexibility of visa programs in light of the interdisciplinary nature of AI and semiconductor R&D.

By making it easier for foreign AI researchers to permanently stay and work in the U.S., the USG could boost domestic AI assets. The current immigration process is already often cumbersome compared to competitors. For example, leading American AI and semiconductor companies, including Google, Microsoft, Apple, Facebook, Intel, and Qualcomm, employ thousands of foreigners and argue that there is a shortage of qualified Americans for scientific and programming jobs.[101] Ian Goodfellow, a top machine learning scientist, said, "visa restrictions have been one of the largest bottlenecks to our collective research productivity over the last few years."[102] In contrast, several other countries like France, the UK, China, and Canada have introduced programs to fast-track visa applications in strategically relevant technology sectors like AI R&D.[103] Notably, after former President Trump announced stricter immigration policies, Baidu chief executive Robin Li Yanhong called on the Chinese government to ease visa restrictions for top tech talent and thereby make it more attractive for AI researchers to come to China.[104] Further, in a 2019 survey of top-tier AI researchers, nearly 70 percent of AI researchers based in the United States considered "visa and immigration issues" a serious problem for AI research in the country, a significantly higher portion than researchers in other countries.[105]

While such measures would likely strengthen domestic AI R&D efforts, they also pose potential risks from the USG's perspective. For instance, increasing the number of foreign professionals in the AI R&D field adds another route that could be exploited by adversaries to steal intellectual property. Expanding green card

---

- Remco Zwetsloot et al., "Keeping Top AI Talent in the United States" (Center for Security and Emerging Technology, December 2019), https://cset.georgetown.edu/wp-content/uploads/Keeping-Top-AI-Talent-in-the-United-States.pdf.
- Will Hunt and Remco Zwetsloot, "The Chipmakers: U.S. Strengths and Priorities in the High-End Semiconductor Workforce" (Center for Security and Emerging Technology, 2020), https://cset.georgetown.edu/research/the-chipmakers-u-s-strengths-and-priorities-for-the-high-end-semiconductor-workforce/.

[100] Also discussed in "Final Report" (National Security Commission on Artificial Intelligence, March 2021), 178, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf

[101] Vindu Goel, "How Trump's 'Hire American' Order May Affect Tech Worker Visas," *The New York Times*, April 18, 2017, https://www.nytimes.com/2017/04/18/technology/h1b-visa-facts-tech-worker.html.

[102] Ian Goodfellow, "I Emphatically Agree. My Collaborators' Visa Restrictions Have Been One of the Largest Bottlenecks to Our Collective Research Productivity over the Last Few Years.," Twitter, February 13, 2019, https://twitter.com/goodfellow_ian/status/1095727254057840640.

[103] Tina Huang and Zachary Arnold, "Immigration Policy and the Global Competition for AI Talent" (Center for Security and Emerging Technology, 2020), https://cset.georgetown.edu/research/immigration-policy-and-the-global-competition-for-ai-talent/.

[104] Meng Jing, "China Must Woo Top Tech Talent Turned off by Trump, Says Baidu Chief," *CNBC / South China Morning Post*, March 6, 2017, https://www.cnbc.com/2017/03/06/china-must-woo-top-tech-talent-turned-off-by-trump-says-baidu-chief.html.

[105] Remco Zwetsloot et al., "The Immigration Preferences of Top AI Researchers: New Survey Evidence" (Perry World House and The Future of Humanity Institute, 2021), https://global.upenn.edu/perryworldhouse/news/immigration-preferences-top-ai-researchers-new-survey-evidence.

access could also backfire. China analyst Matt Sheehan, for example, argues that it could encourage Chinese PhDs to go back to China and seek opportunities there as they would have the security to be able to return to the U.S. at any time. H-1B visas, by contrast, do not incur the same risk since they would incentivize the researchers to stay and work in the U.S. at least for several years.[106]

Under the Trump administration, it was very unlikely that any such measures would have gained the necessary support within the USG. By signing the "Hire American" order, President Trump had criticized the current allocation of H-1B visas to highly qualified foreign workers and argued that more of the positions could be filled by American citizens. However, this calculus might change with the Biden administration. During his first weeks in office, Biden has already launched an overhaul of US immigration law that could make it easier for tech-industry workers and students to come to the United States.[107]

[106] Matt Sheehan, "Who Loses from Restricting Chinese Student Visas?" (MacroPolo, May 31, 2018), https://macropolo.org/who-loses-from-restricting-chinese-student-visas/.
[107] John McCabe, "Biden Vows Immigration Reform to Attract Top Talent to the US," *Science|Business*, January 21, 2021, https://sciencebusiness.net/news/biden-vows-immigration-reform-attract-top-talent-us.

Secrecy Orders

Potential Motives for Use	(1) Deprive a rival of insights into particular AI projects or the AI R&D landscape; (2) Undermine a rival's ability to use AI technologies for national security purposes.
Legislation/Key Documents	Invention Secrecy Act of 1951, Sections 181 to 188 of Title 35, United States Code.
Key Decision-Makers	U.S. Patent and Trademark Office; Defense Agencies; U.S. president.
Affected Actors	All domestic AI R&D actors (subject to potential classification of patent applications).

Table 7: The Invention Secrecy Act Summary

The Invention Secrecy Act, signed by President Truman in 1951, "authorizes the U.S. Patent and Trademark Office (USPTO) to prevent disclosure of the information in patent applications for inventions made in the United States when it considers the publication of this information detrimental to national security."[108] Secrecy orders under the act "block[s] patents from being issued, and, often prohibit the inventors from selling or licensing their technology to anybody but the government."[109] The USPTO's commissioner of patents decides whether to refer an application to a defense agency for review by assessing how damaging to national security the publication of the invention might be. To aid the USPTO in making this determination, defense agencies provide extensive guidance through the (classified) Patent Security Category Review List.[110] Historically, an increasing number of secrecy orders have been imposed on dual-use technologies.[111] Secrecy orders are valid for up to one year, but the commissioner of patents can renew them for another year by the end of each term.[112] If an order is in effect or issued during a national emergency declared by the president, it remains in effect for the duration of the national emergency and six months thereafter.[113]

The number of secrecy orders has been slowly increasing at a constant rate since at least 2005. At the end of 2019, 5,878 secrecy orders were in effect. In 2020, the number of secrecy orders rose to 5,915.[114] So-called

[108] See Eric B. Chen, "Technology Outpacing the Law: The Invention Secrecy Act of 1951 and the Outsourcing of US Patent Application Drafting," *Texas Intellectual Property Law Journal* 13 (2004): 367.
[109] According to Robert E. Garrett, a former director of the Patent and Trademark Office, patents represented "unique 'how to' information," in part because inventors are required by law to fully disclose the details necessary for others to reproduce the invention. Restrictions under the Invention Secrecy Act can block the publication of information developed entirely by individuals who did not receive any government funding. See Edmund L. Andrews, "Cold War Secrecy Still Shrouds Inventions," *The New York Times*, May 23, 1992, https://www.nytimes.com/1992/05/23/business/patents-cold-war-secrecy-still-shrouds-inventions.html.
[110] H.L. Mourning, J.C. Morris, and Bret Convey, "Patent Security Category Review List" (Armed Services Patent Advisory Board, January 1971), https://fas.org/sgp/othergov/invention/pscrl.pdf.
[111] See Appendix A for two examples from the field of cryptography.
[112] G.W. Schulz, "Government Secrecy Orders on Patents Have Stifled More Than 5,000 Inventions," *Wired*, April 16, 2013, https://www.wired.com/2013/04/gov-secrecy-orders-on-patents/.
[113] U.S. Congress, "Secrecy of Certain Inventions and Withholding of Patent," 35 U.S. Code § 181 (1952), https://www.law.cornell.edu/uscode/text/35/181.
[114] Steven Aftergood, "Invention Secrecy Statistics," Federation of American Scientists Project on Government Secrecy, 2020, https://fas.org/sgp/othergov/invention/stats.html.

"John Doe" orders—secrecy orders imposed on private inventors—constitute only a small share of secrecy orders. In 2020, the number of these orders in effect decreased from 48 in 2019 to 21. Violations of a secrecy order by inventors are punished with a fine of up to $10,000 or imprisonment for not more than two years, or both.[115]

The Invention Secrecy Act and AI R&D

By design, secrecy orders would not be disclosed if they were already being used in the context of AI R&D.[116] It can be expected that patent applications covering AI technologies are at least closely monitored by the responsible USG agencies, given the key role that AI has in the DoD's efforts to preserve the US military-technological edge.[117]

Extensive use of secrecy orders is highly unlikely, however. It would very likely clash with the currently open research culture in AI. Even Apple, which had been comparatively secretive about its AI research in the past, has its own online platform to highlight the company's various AI-related research projects.[118] The Invention Secrecy Act is also outdated as it is not applicable to the dissemination of publications on the Internet[119] prior to the filing of a patent application, which could be far more damaging to national security than the patent applications themselves.[120] These factors severely limit the efficacy of this tool from the perspective of the USG, and make it unlikely that it will be widely used in the context of AI R&D. However, these factors are less applicable to semiconductors, where private industry performs most R&D and largely does not publish research.[121] Still, academia is relatively more involved in basic research in emerging hardware approaches, which could play key roles in the future of AI-related computing.[122]

Secrecy orders would also reduce the value of AI and semiconductor companies' patent applications by blocking their issuance. Leading AI companies own thousands of AI patents, with U.S. companies

---

[115] U.S. Congress, "Penalty," 35 U.S. Code § 186 (2011), https://www.law.cornell.edu/uscode/text/35/186.

[116] In 2017, the U.S. had more AI patents than China, with 35,508 versus 34,345 for China. But as Chinese companies and scientists were filing AI patent applications at a faster pace, the nation was likely to hold more AI patents than the U.S. by the end of 2017, according to a report by Sequoia Capital China and Zhen Fund. The U.S. leads in machine learning and natural language processing patents, while China is especially strong in machine vision patents with 55% of the total. See Pan Yue, "China May Own More Artificial Intelligence Patents Than US By Year-End," China Money Network, September 14, 2017, https://www.chinamoneynetwork.com/2017/09/14/china-may-hold-artificial-intelligence-patents-us-year-end.

[117] See for example, U.S. Department of Defense, "Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance our Security and Prosperity", https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF

[118] Jonathan Vanian, "Apple Just Got More Public About Its Artificial Intelligence Plans," *Fortune*, July 19, 2017, https://fortune.com/2017/07/19/apple-artificial-intelligence-research-journal/.

[119] This criticism is only relevant if the technology is not already covered by export control law.

[120] This is of course only the case if the presented technical data is not subject to the ITAR or EAR. See the discussion on deemed exports.
Eric B. Chen, "Technology Outpacing the Law: The Invention Secrecy Act of 1951 and the Outsourcing of US Patent Application Drafting," *Texas Intellectual Property Law Journal* 13 (2004): 352–75, http://www.tiplj.org/wp-content/uploads/Volumes/v13/v13p351.pdf.

[121] See section on "Federal R&D Funding."

[122] For example, academia plays a key role in research in carbon nanotubes. Jason Daley, "Milestone Carbon-Nanotube Microchip Sends First Message: 'Hello World!,'" *Smithsonian Magazine*, August 29, 2019, https://www.smithsonianmag.com/smart-news/advanced-carbon-nanotube-microprocessor-created-180973013/. It also plays a key role in quantum computing research. Matt Swayne, "The World's Top 12 Quantum Computing Research Universities," *The Quantum Daily*, November 18, 2019, https://thequantumdaily.com/2019/11/18/the-worlds-top-12-quantum-computing-research-universities/.

composing four of the top five AI patent holders.[123] Additionally, the U.S. semiconductor industry spends more on R&D as a percentage of revenue than all other major U.S. industries except pharmaceuticals and biotechnology.[124] As a result, several semiconductor companies, including two U.S. companies, Intel and Qualcomm, were among the top twelve U.S. patentees in 2019.[125] The Semiconductor Industry Association says that protecting IP is critical to the U.S. semiconductor industry's competitiveness.[126]

Affected companies and individuals could choose to take costly legal actions if their patent applications were classified. However, inventors of an application which has been placed under a secrecy order usually have limited options to take action against the decision. According to the act, owners have the right to compensation for the use of the technology by the USG and for financial losses incurred.[127] According to a *Bloomberg* article, private inventors who have asked for compensation have rarely been successful due to a catch-22: the inventions are secret and so lack a market because the ideas in the patent applications cannot be publicly revealed. That makes it difficult to demonstrate how much money is being lost by the impact of government secrecy. Therefore, in patent secrecy cases, government lawyers have often argued that there is no evidence that the inventors would have made any money from their ideas.[128] However, while individuals may not have the resources to take costly and enduring legal action against the USG, it is likely that large AI and semiconductor companies would challenge secrecy orders, especially when the presumed economic value of a patent is significant.

---

[123] Martin Armstrong, "Infographic: The Companies With the Most AI Patents," *Statista Infographics*, May 29, 2019, https://www.statista.com/chart/18211/companies-with-the-most-ai-patents/.

[124] "2019 Factbook" (Semiconductor Industry Association, May 2019), 19, https://www.semiconductors.org/wp-content/uploads/2019/05/2019-SIA-Factbook-FINAL.pdf.

[125] Ingrid Lunden, "US Patents Hit Record 333,530 Granted in 2019; IBM, Samsung (Not the FAANGs) Lead the Pack," *TechCrunch*, January 14, 2020, https://social.techcrunch.com/2020/01/14/us-patents-hit-record-333530-granted-in-2019-ibm-samsung-not-the-faangs-lead-the-pack/.

[126] "Winning the Future: A Blueprint for Sustained U.S. Leadership in Semiconductor Technology" (Semiconductor Industry Association, April 2019), 12, https://www.semiconductors.org/wp-content/uploads/2019/04/FINAL-SIA-Blueprint-for-web.pdf. Qualcomm in particular derives massive value from its patent portfolio, obtaining most of its profits from its technology licensing business. "Qualcomm Announces Fourth Quarter and Fiscal 2019 Results" (Qualcomm, November 6, 2019), https://www.qualcomm.com/news/releases/2019/11/06/qualcomm-announces-fourth-quarter-and-fiscal-2019-results.

[127] U.S. Congress, "Right to Compensation," 35 U.S. Code § 183 (2011), https://www.law.cornell.edu/uscode/text/35/183.
The case *Damnjanovic v. U.S. Air Force* (2014/2015) stands out as a rare instance in which the government paid private inventors for a secret patent application. In this case, the inventors Budimir Damnjanovic and Desanka Damnjanovic sought compensation for a secrecy order filed by the U.S. Air Force. The court granted the inventors a lump sum payment of $63,000. "Damnjanovic v. U.S. Air Force," 2015, https://fas.org/sgp/othergov/invention/damn-complaint.pdf.

[128] Joshua Brustein, "Congratulations, Your Genius Patent Is Now a Military Secret," *Bloomberg*, June 8, 2016, https://www.bloomberg.com/news/articles/2016-06-08/congratulations-your-genius-patent-is-now-a-military-secret.

Prepublication Screening Procedures for Security-Sensitive Publications

Potential Motives for Use	(1) Deprive a rival of insights into particular AI projects or the AI R&D landscape (2) Undermine a rival's ability to use AI technology and its core components for national security purposes.
Legislation/Key Documents	National Security Decision Directive 189.
Key Decision-Makers	National Science Foundation, Department of Defense, National Security Agency.
Affected Actors	All U.S. AI R&D actors (to the extent that they are requested to engage in screening).

Table 8: Prepublication Screening Procedure Summary

Prepublication reviews for sensitive research in the U.S. have a long history. During the Cold War, USG concerns over the acquisition of U.S. technology by the Eastern Bloc resulted in a mandatory screening procedure: NSDD-189. The directive "establishes national policy for controlling the flow of science, technology, and engineering information produced in federally funded fundamental research at colleges, universities, and laboratories." Although the directive states that basic research should remain largely unrestricted, it also tasks federal agencies with "a) determining whether classification is appropriate prior to the award of a research grant, contract, or cooperative agreement and, if so, controlling the research results through standard classification procedures; b) periodically reviewing all research grants, contracts, or cooperative agreements for potential classification." Current USG concerns over technology transfers to China have revitalized debates around the scope, opportunities, and challenges of NSDD-189, which, while not used actively, remains in place.[129]

A voluntary prepublication review procedure for a specific discipline was first introduced in the 1980s, in the field of cryptography research (see Appendix A for further details). In 1979, then NSA Director Vice Admiral B.R. Inman publicly voiced his concern that some information contained in published articles on cryptography endangered the mission of the NSA, and thus U.S. national security.[130] The USG had become

[129] Mary Sue Coleman, "Balancing Science and Security," *Science* 365, no. 6449 (July 12, 2019): 101–101, https://doi.org/10.1126/science.aay5856.

[130] See Appendix A for a more thorough discussion of the subsequent efforts. Bobby R. Inman, "The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector," *Cryptologia* 3, no. 3 (1979): 129–135, https://doi.org/10.1080/0161-117991853954.
Until then, the NSA did not have statutory power to require the submission of proposed publications for prior review or to require changes in publications prepared outside the agency and not under NSA contract or grant. However, the National Science Foundation announced during the process that it had responsibility under routine executive orders to refer to the NSA information developed in NSF-sponsored research projects on cryptologic research that it believes may be classifiable. See Jonathan Knight, "Cryptographic Research and NSA," *Academe* 67, no. 6 (1981): 375, https://doi.org/10.2307/40248881.
In its current policy, the NSF states: "NSF grants are intended for unclassified, publicly releasable research. The grantee will not be granted access to classified information. NSF does not expect that the results of the research project will involve classified information. If, however, in conducting the activities supported under a grant, the PI/PD is concerned that any of the research results involve potentially classifiable information that may warrant Government restrictions on the dissemination of the results, the PI/PD should promptly notify the cognizant NSF Program

concerned that open publication of research results in cryptography could reveal vulnerabilities in encryption algorithms that an enemy could exploit.[131] The most significant problem was the possibility that a "blockbuster paper"—one reporting on research constituting a significant scientific breakthrough—might slip through the system and seriously damage U.S. national security.[132] In 1980, the American Council on Education convened the Public Cryptography Study Group (PCSG), which eventually recommended the introduction of a system in which the NSA would invite authors of specific papers to submit cryptography manuscripts for prior review at the same time that the manuscripts were submitted for publication. The NSA was to define the exact research areas covered by the system, and manuscripts had to be returned promptly to the authors with explanations and recommendations in case of any national security concerns. With the support of all except one member, the PCSG accepted the proposal. Neither the research community nor the NSA were entirely satisfied with the review system. However, the implementation of the review procedure eased fears about impounded research and unnecessary constraints as there have been only a few NSA requests for prepublication review. In some cases, the NSA required minor changes. In a few instances, they asked scientists to hold back research results. In other cases, the NSA helped researchers to lift or avoid secrecy orders imposed on cryptography research (see Appendix A for more details).[133]

Another illustrative example comes from the field of biotechnology. The USG set up the National Science Advisory Board for Biosecurity (NSABB) in 2004 to address issues related to biosecurity and dual-use research. The NSABB has up to 25 voting members with a broad range of expertise including molecular biology, national security, law enforcement, and scientific publishing. Notably, in 2011, the NSABB recommended restricting the content of two scientific papers concerning the laboratory adaptation of the avian H5N1 influenza virus to mammal-to-mammal respiratory transmission in order to prevent others from replicating their work. The recommendation was considered to be unprecedented for work in the life sciences.[134]

Prepublication Screening Procedures and AI R&D

Following previous models, the USG may consider introducing a publication screening procedure for research in AI with potential national security concerns. This measure would not necessarily require new legislation, since NSDD-189 remains active and therefore in theory also applies to federally funded AI R&D projects at colleges, universities, and in laboratories. For research without federal funding, the USG could implement a voluntary screening procedure similar to that in cryptography. The USG would have to come up with a model for the prepublication review, such as the NSABB in the case of biotechnology or a

---

Officer." See "Proposal and Award Policies and Procedures Guide" (National Science Foundation, January 30, 2017), 133, https://www.nsf.gov/pubs/policydocs/pappg17_1/nsf17_1.pdf.

[131] National Academy of Engineering, "Appendix E: Voluntary Restraints on Research with National Security Implications: The Case of Cryptography, 1975-1982," in *Scientific Communication and National Security* (Washington, DC: The National Academies Press, 1982), https://doi.org/10.17226/253.

[132] In August 1989, over the objections of the NSA, the computer scientist John Gilmore distributed a paper, written by Robert Merkle, describing fast and inexpensive ways of keeping computer information private. See John Markoff, "Paper on Codes Is Sent Despite U.S. Objections," *The New York Times*, August 9, 1989, https://www.nytimes.com/1989/08/09/us/paper-on-codes-is-sent-despite-us-objections.html.

[133] See section above on the "Invention Secrecy Act" for further information.
Lance J. Hoffman, *Building in Big Brother: The Cryptographic Policy Debate* (New York: Springer, 1995).

[134] National Institutes of Health (NIH), "Press Statement on the NSABB Review of H5N1 Research," September 18, 2015, https://www.nih.gov/news-events/news-releases/press-statement-nsabb-review-h5n1-research. For a good overview of the case, also see Gigi Kwik Gronvall, "H5N1: A Case Study for Dual-Use Research" (Council on Foreign Relations, 2013), https://www.centerforhealthsecurity.org/our-work/publications/h5n1-a-case-study-for-dual-use-research.

procedure administered by a USG agency like the NSA in the case of cryptography. The USG would need to collaborate with key representatives of the AI research communities; it could initiate and coordinate the process, but, ultimately, it is restricted in its capacity to enforce compliance for research that is not federally funded.

At present, there are no signs that the USG is considering initiating such prepublication screening procedures for AI R&D. Indeed, there are to date few if any cases of AI research that the USG would have had an interest in blocking publication of. Furthermore, several features of the AI field render the implementation of such a prepublication procedure difficult, which decreases the probability that such a system will be implemented in the near future. First, the research community seems divided about whether the publication of any forms of AI research currently poses significant national security risks. Therefore, it might be difficult to gain enough support from key representatives of the community for such a measure. Second, AI R&D is a quickly expanding field and many new findings are near-instantly published online, making review and monitoring more challenging than it historically has been for the field of cryptography. Third, AI researchers and companies have established a very open research culture; accepting a ban on or delaying publishing research results would run counter to that culture.

The USG may also face difficulty applying a prepublication screening procedure to hardware R&D. NSDD-189 could apply to USG-funded research into semiconductors and emerging hardware. However, the USG accounts for only 4% of U.S. semiconductor R&D funding.[135] As such, the vast majority AI-related hardware R&D would be immune to such a procedure.

[135] See section on "Federal R&D Funding."

The Defense Production Act

Potential Motives for Use	Make/keep relevant AI technologies available for national security purposes.
Legislation/Key Documents	Defense Production Act of 1950, as amended.
Key Decision-Makers	President of the United States, Department of Commerce (Bureau of Industry and Security), Department of Defense (Defense Production Act Title III Office).
Affected Actors	U.S. AI developers and researchers (volunteering for National Defense Executive Reserve).

Table 9: The Defense Production Act Summary

The Defense Production Act (DPA) of 1950, as amended, confers upon the president a broad set of authorities to require private companies to supply products, materials, and services in the interest of the "national defense."[136] The president has historically delegated his powers under the DPA to department and agency heads via executive orders. The authorities can be used across the federal government to shape the domestic industrial base so that, when called upon, it is capable of providing essential materials and goods needed for national defense. Though initially passed in response to the Korean War, the DPA is historically based on the War Powers Acts of the Second World War. Gradually, Congress has expanded the term "national defense" as defined in the DPA. The scope of DPA authorities now extends beyond shaping U.S. military preparedness and capabilities, as the authorities may also be used to enhance and support domestic preparedness, response, and recovery from natural hazards, terrorist attacks, and other national emergencies.[137] Some current DPA authorities include but are not limited to:

> *Title I*: Priorities and Allocations, which allows the president to require persons (including businesses and corporations) to prioritize and accept contracts for materials and services as necessary to promote the national defense.
>
> *Title III*: Expansion of Productive Capacity and Supply, which allows the president to incentivize the domestic industrial base to expand the production and supply of critical materials and goods. Authorized incentives include loans, loan guarantees, direct purchases, and purchase commitments as well as the authority to procure and install equipment in private industrial facilities.
>
> *Title VII*: General Provisions, which includes key definitions for the DPA and several distinct authorities, including the authority to establish voluntary agreements with private industry and the authority to block proposed or pending foreign corporate mergers, acquisitions, or takeovers that threaten national security. These authorities are the basis for CFIUS as discussed previously in the

[136] The DPA frequently expires and requires reauthorization, at which point it can be amended in various ways. It was last reauthorized in 2019 and next expires in 2025.
[137] Notably, the DPA was recently triggered to support the response to the coronavirus pandemic (COVID-19). See, e.g., Michael H Cecire and Heidi M Peters, "The Defense Production Act (DPA) and COVID-19: Key Authorities and Policy Considerations" (Congressional Research Service, March 18, 2020), https://fas.org/sgp/crs/natsec/IN11231.pdf.

section on Foreign Investment Restrictions. Title VII also allows the president to employ persons of outstanding experience and ability and to establish a volunteer pool of industry executives who could be called to government service in the interest of national defense. This volunteer pool is called the National Defense Executive Reserve and was originally established through Executive Order 11179 in 1964.

The Defense Production Act and AI R&D

Given that the applicability of DPA Title VII authorities to Foreign Investment Reviews were discussed previously, this section focuses on Title I, Title III, and, with respect to the National Defense Executive Reserve (NDER), Title VII. In short, the use of the DPA with regards to AI seems unlikely.

In the case of AI software and research, it is difficult to imagine why or how the USG would use Titles I and III. These titles are primarily used for targeting supplies where quantity and production capacity matters. However, these metrics are more relevant to the supply of AI-relevant hardware. In some unlikely scenarios, the USG may be unable to procure specialized AI chips from private companies for specific national security use cases. For example, commercial AI-specific chips may be inefficient for USG applications or made of materials ill-suited for military or space applications. Under such scenarios, the USG could use the DPA to compel semiconductor companies to prioritize the design and manufacture of specialized chips to serve their purposes. It could also use the DPA to prioritize the USG's use of private data centers or supercomputers.

Under DPA Title VII, the USG could face difficulty recruiting key AI researchers and engineers onto the National Defense Executive Reserve (NDER) and requiring them to support AI projects prioritized by the government. For one, researchers would have to join voluntarily since the procedure for reservists to join the NDER is by application. Further, even at the height of the Cold War, the NDER was found to be a weak instrument, as it was underfunded, poorly administered, and unevenly implemented by different agencies.[138] [139]

[138] Donald Horan, "National Defense Executive Reserve Program" (U.S. General Accounting Office), accessed June 18, 2020, https://www.gao.gov/assets/210/206264.pdf.

[139] We are grateful to Michael Page for sharing his thoughts on the applicability of the Defense Production Act to AI R&D.

Antitrust Enforcement

USG Goals	(1) Strengthen domestic AI and semiconductor industries; (2) Make/keep relevant AI technologies available for national security purposes.
Legislation/Key Documents	Sherman Antitrust Act; Clayton Antitrust Act; Robinson-Patman Act; FTC Act.
Key Decision-Makers	Department of Justice, Federal Trade Commission, private litigants, U.S. Supreme Court.
Affected Actors	Large AI and semiconductor companies.

Table 10: Antitrust Enforcement Summary

While antitrust law usually regulates anticompetitive behavior between private economic actors (both businesses and individuals),[140] the USG has used antitrust as a strategic lever in the past.[141] In particular, it has tried to either promote competition in the development and sale of strategic commodities or protect strategically helpful firms. American antitrust authorities are well-funded and have the ability to seek large civil and criminal penalties for violations of antitrust law. They also retain significant discretion in choosing which cases to pursue.

American antitrust law emerged in the late 1800s as a response to newfound concentrations of power in the American economy. The modern antitrust regime spans a number of different statutes at the national and, less importantly, state levels.[142] Since the late 1970s, the dominant view, associated with the Chicago school of law and economics, has been that the sole purpose of antitrust is the promotion of well-functioning, efficient markets by preventing firms from engaging in conduct that harms consumer welfare as measured economically.[143]

The USG has a number of possible remedies available to it in successful antitrust actions, including damages and injunctions.[144] Perhaps the most drastic measure is divestiture: forcing a monopolistic firm to split up or sell assets to restore competition. Such remedies give the USG obvious leverage over firms with antitrust

[140] See Christopher J. MacAvoy, "US Antitrust Laws: Overview," Practice Note 9-204-0472, Practical Law, 2018.
[141] For examples of how the U.S. has used antitrust to promote geostrategic goals, see Cullen O'Keefe, "How Will National Security Considerations Affect Antitrust Decisions in AI? An Examination of Historical Precedents" (Future of Humanity Institute, University of Oxford, 2020), https://www.fhi.ox.ac.uk/antitrust-okeefe.
[142] See Appendix B.
[143] See Maurice E. Stucke, "Reconsidering Antitrust's Goals," *Boston College Law Review* 53 (2012): 551, 556, 563–66, https://lawdigitalcommons.bc.edu/bclr/vol53/iss2/4/.; Christine S Wilson, "Welfare Standards Underlying Antitrust Enforcement: What You Measure Is What You Get" (Arlington, VA: Federal Trade Commission, February 15, 2019), https://www.ftc.gov/system/files/documents/public_statements/1455663/welfare_standard_speech_-_cmr-wilson.pdf.; "Public Interest Considerations in Merger Control: Note by the United States" (Directorate for Financial and Enterprise Affairs, June 2, 2016), https://perma.cc/XB26-CRTP.
[144] See Appendix B.

liability,[145] but legal norms constrain the USG's ability to exploit that leverage for geostrategic purposes beyond maintaining competitive markets generally.[146]

The USG can also settle antitrust cases through consent decrees.[147] Importantly, under the Tunney Act, a federal judge must approve antitrust consent decrees as being in the "public interest."[148] It is unclear whether national security considerations can enter into that analysis.[149] Thus, the USG's ability to use consent decrees for geostrategic purposes beyond maintaining competitive markets generally remains untested.

Antitrust Enforcement and AI R&D

In the context of AI R&D, the USG could decide to use a variety of antitrust measures. On the one hand, stricter antitrust scrutiny of large AI or semiconductor companies could stimulate competition between a larger number of firms.[150] This might foster higher levels of innovation.[151] It could also lower the USG's procurement costs and reduce suppliers' bargaining power against the USG.[152] While some major U.S. politicians, out of concern for consumers, have recently been calling for the increased scrutiny of big tech firms with AI businesses,[153] such firms have largely avoided having to divest any major assets to date. Nevertheless, the possibility of significant changes to antitrust law has become increasingly salient.[154]

By comparison, to promote competition, the USG has frequently filed antitrust actions in recent years against major semiconductor companies including chipmaker Intel,[155] equipment maker Applied

---

[145] See generally Cullen O'Keefe, "How Will National Security Considerations Affect Antitrust Decisions in AI? An Examination of Historical Precedents" (Future of Humanity Institute, University of Oxford, 2020), https://www.fhi.ox.ac.uk/antitrust-okeefe.

[146] See James F. Rill and Stacy L. Turner, "Presidents Practicing Antitrust: Where to Draw the Line," *Antitrust LJ* 79, no. 2 (2014): 577, https://www.jstor.org/stable/43486917.

[147] "A court order to which all parties have agreed. It is often done after a settlement between the parties that is subject to approval by the court." "Consent Decree," Wex, accessed June 13, 2018, https://www.law.cornell.edu/wex/consent_decree.

[148] See Appendix B.

[149] See United States v. American Tel. and Tel. Co., 552 F. Supp. 131, 149, 149 n.77, Civ. A. No. 74-1698 (D.D.C. 1982).

[150] See Appendix B for an example of this with other defense-relevant technologies (Union Pacific, I.G.).

[151] Cf. Dakota Foster and Zachary Arnold, "Antitrust and Artificial Intelligence: How Breaking Up Big Tech Could Affect the Pentagon's Access to AI" (Center for Security and Emerging Technology, 2020), https://doi.org/10.51593/20190025.

[152] "Three South Korean Companies Agree to Plead Guilty and to Enter into Civil Settlements for Rigging Bids on United States Department of Defense Fuel Supply Contracts," Press Release (Department of Justice, November 14, 2018), https://perma.cc/7922-UU28. "'The Antitrust Division has a long history of vigilantly protecting the interests of American consumers through civil and criminal antitrust enforcement. Going forward, it is my goal to apply that same vigilance to protect the interests of American taxpayers,' [said Assistant Attorney General Makan Delrahim of the Department of Justice's Antitrust Division]."

[153] See Elizabeth Warren, "Here's How We Can Break up Big Tech," October 11, 2019, https://medium.com/@teamwarren/heres-how-we-can-break-up-big-tech-9ad9e0da324c; cf. House Subcommittee on Antitrust, Commercial and Administrative Law, "Investigation of Competition in Digital Markets: Majority Staff Report and Recommendations," 2020, https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf.

[154] See House Subcommittee on Antitrust, supra.

[155] "Intel Corporation, In the Matter Of" (Federal Trade Commission, November 2, 2010), https://www.ftc.gov/enforcement/cases-proceedings/061-0247/intel-corporation-matter.

Materials,[156] and chip designers Qualcomm[157] and Broadcom.[158] Largely due to natural economic forces, the semiconductor industry has continually consolidated over the past decades.[159] The small number of remaining companies at the state-of-the-art in several semiconductor supply chain segments could make the USG especially vigilant about future perceived anticompetitive behavior.[160]

On the other hand, the USG could act leniently to protect an industry player that aids USG national security interests. Firms could argue that antitrust actions would disrupt important security-relevant operations, for example.[161] Big American tech firms have often argued that their size is an asset to American interests insofar as it allows them to counterbalance the influence of large foreign (especially Chinese) firms.[162] This would incentivize those firms to continue serving the USG's interests.

There are also more speculative and controversial uses, which are significantly less likely but have more far-reaching consequences. The USG would probably only consider using them in a severe national security crisis. For example, the USG could use antitrust as a tool to achieve national security objectives unrelated to the conduct that triggered the antitrust action, e.g., by targeting AI developers or semiconductor companies that are both aiding an adversary and engaging in anticompetitive conduct. The USG could also try to gain access to intellectual property in AI or semiconductors via antitrust consent decrees.[163] Such uses would likely require very strong national security justifications, would be politically controversial, are legally suspect, and would most probably lead to an open conflict with the AI and semiconductor industries.[164]

The prospect of potential antitrust action is a lever in itself. Recent events have shed light on how important it is for big tech companies to avert antitrust action and to cultivate a good relationship with the USG. Large firms are heavily dependent on a good relationship with the USG[165] to flourish in the U.S. market but also to have favorable conditions when operating in foreign markets. They go to great lengths to build such relationships. According to *The Guardian*, Google spent $5.93 million trying to lobby elected officials in

---

[156] "Applied Materials Inc. and Tokyo Electron Ltd. Abandon Merger Plans After Justice Department Rejected Their Proposed Remedy" (Department of Justice, April 27, 2015), https://www.justice.gov/opa/pr/applied-materials-inc-and-tokyo-electron-ltd-abandon-merger-plans-after-justice-department.

[157] "Qualcomm Inc." (Federal Trade Commission, November 25, 2019), https://www.ftc.gov/enforcement/cases-proceedings/141-0199/qualcomm-inc.

[158] "Broadcom Limited/Brocade Communications Systems, In the Matter Of" (Federal Trade Commission, July 12, 2017), https://www.ftc.gov/enforcement/cases-proceedings/171-0027/broadcom-limitedbrocade-communications-systems.

[159] These forces include economies of scale, rising capital costs, and the clustering of talent to support transmission of implicit know-how.

[160] For example: only Intel, Samsung, and TSMC run state-of-the-art chip fabs; Applied Materials, Lam Research Tokyo Electron, and ASML capture about two-thirds of semiconductor manufacturing equipment revenue; only Nvidia and AMD sell advanced discrete GPUs; Intel and Xilinx dominate the FPGA market; and Synopsys, Cadence Design Systems, Mentor Graphics, and Ansys capture about 90% of the electronic design automation (EDA) market.

[161] See O'Keefe, supra at 11-13.

[162] See O'Keefe, supra, at 35.

[163] See O'Keefe, supra at 8-10.

[164] See O'Keefe, supra. Additionally, the USG may better accomplish its goals using other levers, for example, by applying export controls to prevent U.S. companies from aiding adversaries.

[165] Mark Bergen, Sarah Frier, and Selina Wang, "Google, Facebook, Twitter Scramble to Hold Washington at Bay," *Bloomberg*, October 10, 2017, https://www.bloomberg.com/news/articles/2017-10-10/google-facebook-and-twitter-scramble-to-hold-washington-at-bay.

Washington during the second quarter of 2017, more than any other corporation.[166] In response to antitrust allegations, companies have argued that their dominance is hardly endurable, given that market entry barriers for competitors are very low. Google's Eric Schmidt, for example, has repeatedly said that "competition is just one click away."[167] Moreover, companies have been arguing that they are successful primarily because of the quality of their offerings and that adopting antitrust measures would therefore lower consumer welfare.[168]

As emphasized before, there is a mutual dependency between technology firms and the USG. While the USG continues to depend on technology firms as national innovation powers, the firms heavily depend on the USG to operate without major constraints in the U.S. market as well as abroad. The USG could therefore use its influence by threatening AI companies with antitrust enforcement or, more drastically, changes to antitrust law. Technology companies will likely continue to invest heavily in preventing antitrust charges through extensive lobbying campaigns[169] and other ways of influencing key decision-makers.[170]

While the changes in antitrust legislation currently being considered by Congress[171] are unlikely to introduce explicit national security considerations into its enforcement, a broadened framework for antitrust analysis may still have national security implications. However, it is unclear whether such changes would promote USG national security interests. For example, though a more competitive AI industry might increase USG access to AI technology,[172] some claim it could reduce the ability for companies to innovate and remain globally competitive.[173]

---

[166] Jonathan Taplin, "Why Is Google Spending Record Sums on Lobbying Washington?," *The Guardian*, July 30, 2017, https://www.theguardian.com/technology/2017/jul/30/google-silicon-valley-corporate-lobbying-washington-dc-politics.
Brian Fung and Hamza Shaban, "Want to Understand How Dominant Tech Companies Have Become? Look at the Number of Issues They Lobby On.," *Washington Post*, August 31, 2017, https://www.washingtonpost.com/news/the-switch/wp/2017/08/31/want-to-understand-how-dominant-tech-companies-have-become-look-at-the-number-of-issues-they-lobby-on/.

[167] "Schmidt on Antitrust: Competition Is One Click Away," *NBC Bay Area*, September 21, 2011, https://www.nbcbayarea.com/news/national-international/schmidt-on-antitrust-competition-is-one-click-away/1901637/.

[168] For example: Bill Gates, "We're Defending Our Right to Innovate," *Wall Street Journal*, May 20, 1998, https://www.wsj.com/articles/SB895616628927103500.

[169] Fung and Shaban, "Want to Understand How Dominant Tech Companies Have Become?"

[170] Kenneth P. Vogel, "New America, a Google-Funded Think Tank, Faces Backlash for Firing a Google Critic," *The New York Times*, September 1, 2017, https://www.nytimes.com/2017/09/01/us/politics/anne-marie-slaughter-new-america-google.html.

[171] See House Subcommittee on Antitrust, supra.

[172] Dakota Foster and Zachary Arnold, "Antitrust and Artificial Intelligence: How Breaking Up Big Tech Could Affect the Pentagon's Access to AI" (Center for Security and Emerging Technology, 2020), https://doi.org/10.51593/20190025.

[173] Emily Stewart, "Facebook's Latest Reason It Shouldn't Be Broken up: Chinese Companies Will Dominate," *Vox*, May 20, 2019, https://www.vox.com/recode/2019/5/20/18632669/sheryl-sandberg-break-up-facebook-china-cnbc.
Teece, D.J., Pisano, G. and Shuen, A., "Dynamic capabilities and strategic management," *Strat. Mgmt. J.*, no. 18 (1997): 509-533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z

The "Born Secret Doctrine"

Potential Motives for Use	(1) Deprive a rival of insights into particular AI projects or the AI R&D landscape; (2) Undermine a rival's ability to use AI technologies for national security purposes.
Legislation/Key Documents	Atomic Energy Act of 1946 & 1954.
Key Decision-Makers	U.S. Department of Energy.
Affected Actors	Domestic AI R&D actors (subject to classification of AI R&D).

Table 11: The "Born Secret Doctrine" Summary

The "Born Secret Doctrine" is a unique feature of American law, as it affects all public discussion of an entire subject matter. During the Second World War, research on nuclear weapons was conducted in secret by the Manhattan Project. Following the end of the war, Congress started negotiations on how to reorganize control over nuclear science. The resulting bill, the Atomic Energy Act, included what is now known as the "Born Secret Doctrine." It introduced a pervasive system of governmental secrecy and control for all R&D information related to nuclear weapons design and testing as well as certain research on the production of nuclear power. Under the act, all information that is deemed relevant to the production of nuclear weapons, the production of special nuclear material, and the use of special nuclear material in the production of energy is "born classified." This implies that even research done outside the national laboratories under private sponsorship is automatically classified and belongs to the government.[174]

A Born Secret Doctrine and AI R&D

While we consider it highly improbable that such a law would ever be developed in the context of AI, we still opted to include it to show the full spectrum of levers that have been used by the USG in the past, ranging to far-reaching controls like the "Born Secret Doctrine." Adopting such a law would be a fairly radical step. While, in theory, it might be possible to prevent the diffusion of certain forms of AI research with such restrictions, the practical implementation would be very difficult, costly, and trigger considerable resistance.

Firstly, the "Born Secret Doctrine" was introduced at a point in time when sensitive nuclear research was government funded and until then had been conducted in secret by the Manhattan Project. These conditions supported the implementation and acceptance of the "Born Secret Doctrine" concerning nuclear research.[175] The fields of AI and hardware R&D, however, are structured very differently. The most cutting-edge research is privately funded and conducted largely by companies. The U.S. semiconductor industry performs 96% of U.S. semiconductor R&D.[176] Secondly, as mentioned before with regard to other levers, strict limitations on AI R&D implemented by the USG would run strongly counter to the open and international research culture of the AI community. The challenges may be even greater if applied to the

[174] National Research Council (US) Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, "Information Restriction and Control Regimes," in *Biotechnology Research in an Age of Terrorism* (Washington, DC: National Academies Press (US), 2004), https://www.ncbi.nlm.nih.gov/books/NBK222057/.
[175] See Appendix C for more details.
[176] See section on "Federal R&D Funding."

semiconductor industry. Semiconductor supply chains are highly globalized, such that many steps in the production of AI-relevant chips are typically performed outside the United States, including chip fabrication. Some key inputs to chip manufacturing, such as advanced photolithography equipment, are only produced by non-U.S. firms. Localizing these supply chains to prevent disclosure to foreign countries would impose great costs and damage U.S. firms' abilities to produce advanced chips.

If such secrecy measures were introduced, it is very likely that researchers would challenge them under the First Amendment[177] and AI and semiconductor companies would either press legal charges to recoup economic losses or consider leaving the U.S. to continue operations in a more favorable regulatory environment. Indeed, even the "Born Secret Doctrine" faced significant public backlash despite the very different political conditions at the time (see Appendix C for details). All of these factors make the introduction of such a doctrine exceedingly costly and very unlikely barring a national security crisis.

[177] See Appendix C.

Conclusion

This section includes estimates of the likelihood of levers being used, a summary assessment of the various policy levers, and a list of further research questions.

Comparative Likelihood Assessment

How likely is the USG is to use the levers covered in this report in the context of AI? The USG is already taking advantage of some of them. For example, it has taken steps to increase federal R&D funding for AI, a trend that is likely to continue under a Biden administration. It has also tightened restrictions on foreign investment through FIRRMA, which seems to have already decreased foreign acquisitions of domestic firms developing AI technologies. Export controls on some AI technologies are already in place, and the USG is considering further expansions. Visa vetting for foreign AI and semiconductor professionals and researchers seems to have increased recently, based on longer waiting times and declining approval rates.

With respect to other levers, it is unclear whether the USG is already using them in the context of AI. In the case of the Invention Secrecy Act, we simply cannot know whether some patent applications for AI technologies have been classified by the USG. It seems unlikely, however, that the USG is doing so on a large scale, since secrecy orders are rare and since we expect this practice would not stay secret for long. We expect the use of both levers to increase with the heightening of general national security concerns and, in particular, the further consideration of AI as relevant to those concerns.

The remaining levers are not yet used in the context of AI. Notably, several groups, including from the AI and semiconductor industries, are already calling for expanded visa pathways to meet talent shortages. It thus seems likely that the USG will seek to balance any increased visa-vetting measures with addressing the talent needs of its domestic AI and semiconductor industries. The likelihood of major changes, however, will depend on the Biden administration; the Trump administration was strongly opposed to increasing the inflow of foreign workers. Voluntary screening procedures for AI publications would require significant buy-in and trust from the domestic AI researcher community. We do not foresee such a collaboration without concrete and compelling threats to national security. Use of the Defense Production Act or antitrust action for national security ends would require significantly heightened national security concerns. They come with significant costs, and the USG has little obvious reason to use them today.

Summary Assessment of Policy Levers

Goal Pursued	Policy Levers
Strengthen the domestic AI industry	• Federal R&D funding providing capital • Expanded visa pathways addressing talent gaps • Antitrust lawsuits stimulating competition, or lenient action on antitrust to protect national security interests • Reductions in foreign direct investment restrictions
Weaken a rival's domestic AI industry	• Foreign investment restrictions depriving companies from rival countries of investment opportunities • Export controls depriving companies from rival countries of imports • Expanded visa pathways (indirectly) encouraging foreign talent to work in the U.S. (as opposed to a rival country) • Restricted visa pathways (indirectly) reducing espionage and flow of tacit knowledge to other countries
Make/keep relevant AI technology and its core components available for national security purposes	• Federal R&D funding giving (at least some) access to intellectual property • Select antitrust lawsuits, e.g., via consent decrees • Defense Production Act recruiting a voluntary National Defense Executive Reserve that can be called on for national security purposes
Undermine a rival's ability to use AI technology and its core components for national security purposes	• Foreign investment restrictions preventing acquisition of or access to intellectual property and talent • Export controls preventing acquisition of critical technology or intellectual property, including technical data • Visa vetting preventing access of foreign nationals to critical technology, know-how, or intellectual property • Voluntary screening procedures limiting access to sensitive research insights or intellectual property • Invention Secrecy Act limiting access to sensitive research insights or intellectual property • Born Secret Doctrine limiting access to sensitive research insights or intellectual property
Gain insights into the AI R&D landscape	• Federal R&D funding to gain information on and access to cutting-edge research
Deprive a rival of insights into the AI R&D landscape	• Foreign investment restrictions preventing acquisition of or access to intellectual property and talent • Visa vetting preventing access of foreign nationals to critical technology, know-how, or intellectual property • Voluntary screening procedures limiting access to sensitive research insights or intellectual property • Invention Secrecy Act limiting access to sensitive research insights or intellectual property • Born Secret Doctrine limiting access to sensitive research insights or intellectual property

Table 12: Levers by Goal Pursued

Potential Barriers or Downsides	Levers
Backlash or increased friction with private AI actors	• Voluntary screening procedures • Defense Production Act (recruiting a voluntary National Defense Executive Reserve) • Invention Secrecy Act • Born Secret Doctrine • Antitrust lawsuits
Increased espionage	• Expanded visa pathways allowing foreign nationals more access to U.S. AI companies
Legal challenges	• Invention Secrecy Act • Born Secret Doctrine • Antitrust lawsuits
Weakening of domestic AI industry	• Foreign investment restrictions by depriving domestic actors of access to capital • Export controls by depriving of export opportunities • Visa vetting by depriving of access to labor • Antitrust lawsuits • Born Secret Doctrine • Invention Secrecy Act
Foreign policy costs (which could undermine international cooperation)	• Foreign investment restrictions causing retaliatory policies and undermining trust • Export controls causing retaliatory policies and undermining trust

Table 13: Levers by Potential Downside

Further Research Questions

Building on this report, further lines of research that could be of high value to pursue can be clustered into four main themes: 1) expanding on government AI R&D policy levers, 2) identifying and analyzing the possible levers of American AI and semiconductor companies, 3) identifying and analyzing the policy levers of other governments, especially the Chinese government and the EU, with regards to their AI and semiconductor industries and other relevant actors, and 4) exploring the levers of non-American AI and semiconductor companies in turn.

1) Further investigation into the USG's AI R&D policy levers

1. What tools other than the ones discussed in this report could the USG use to exert influence over AI R&D?
    a. What variants of the levers mentioned in this report could be relevant?
        i. For example, other aspects of patent law aside from the Invention Secrecy Act could be relevant (e.g., patent-eligibility laws, international IP protection).

        ii. Other forms of information control aside from export controls and voluntary screening procedures may be relevant (e.g., the management of Controlled Unclassified Information).
    b. What formal policy levers have not been discussed in this report, but warrant further investigation? (e.g., certification and accreditation of technologies; standards for testing, evaluation, verification, and validation (TEVV); technology standards and benchmarking; requirements specified in federal acquisition contracts)
    c. What informal and/or indirect policy levers could the USG exert over private R&D activities? (e.g., tax incentives, government purchasing power)
2. What changes could affect the relative likelihood of each of the policy levers mentioned in this report being used by the USG, and the relative efficacy of each lever in achieving the USG's goals?
    a. What can we learn from historical case studies where the USG sought to influence the development of strategic technologies?
3. What new legislation could potentially be enacted under more extreme circumstances to exert greater degrees of influence over private R&D activities?
    a. What precedents do we have of such circumstances occurring, and what can we learn from examining these events?

2) Identifying and analyzing the policy levers of American AI and semiconductor companies

4. How might industry shape/deter/resist levers used by the USG?
    a. What are the primary determinants of firms' stances toward government controls? (e.g., public opinion, leadership, proximity of product to defense applications, basic vs applied research focus)
    b. What are past cases where similar industries actively shaped the design of new legislation or resisted pressure by the USG?
5. Why and how is the industry already pushing back against specific measures targeting AI and semiconductor R&D?
    a. What range of reactions have we seen from different actors?
    b. What actions have the USG taken to assuage industry concerns, if any?
6. What policy levers do AI and semiconductor companies have over the USG to shape AI R&D according to their preferences?
    a. What levers do firms already use? How likely is it that firms will make use of other levers?

3) Identifying and analyzing the policy levers of other governments over relevant AI R&D actors

7. What policy levers do other governments, particularly the Chinese government and the EU, have to control AI R&D? What measures are being discussed or have already been introduced?
8. What are the main differences between the U.S. "toolbox" and the "toolboxes" of other countries? What are the main differences in how these toolboxes are being used or might be used in the future?
9. What policy levers could other governments, in particular the Chinese government and the EU, exercise with regards to American AI and semiconductor companies? How could these interact with policy levers exercised by the USG?

4) Exploring the policy levers of non-American AI and semiconductor companies

10. What tools do non-American AI companies, particularly Chinese companies, have to shape their government's actions according to their preferences? What levers do firms already use? How likely is it that firms will make use of other levers?
11. How can non-American AI and semiconductor companies shape the policy levers used by their governments?
12. What are the main differences between the tools available to American and non-American AI and semiconductor firms? What are the main differences in how these levers are being used or might be used in the future?

Appendix A: Cryptography: A Case Study

Why is Cryptography of National Security Relevance?

Cryptographic technologies can enable malicious behavior because encryption allows adversarial actors to hamper efforts to stop them and cryptanalysis techniques can enable cyberattacks.

Adversarial actors, whether they be hostile states, terrorist groups, or criminals, can use encryption to conceal information and avoid detection by law enforcement and intelligence agencies. According to U.S. administration officials, cryptographic technology in the hands of foreign adversaries has harmed national security interests by impairing intelligence gathering efforts, increasing the capabilities of adversaries to conceal the development of missile delivery systems and weapons of mass destruction, and increasing the costs of national security operations. Similarly, Deputy Attorney General Rod Rosenstein claimed that in 2017, because of encryption, "the FBI was unable to access about 7,500 mobile devices submitted to its Computer Analysis and Response team, even though there was the legal authority to do so."[178] As cryptographic technologies become more widespread, the challenge will only be exacerbated. A recent study assesses that 47% of smartphones and tablets in the U.S. have full disk encryption, and that by 2019, 22% of the total traffic on mobile messaging applications would be unrecoverable to law enforcement agencies.[179] There have been several recorded instances of terrorist groups such as Al-Qaida and the Islamic State using encryption to deliberately evade capture, making this barrier to law enforcement particularly salient.[180]

Cryptanalysis techniques—methods for decrypting encrypted data—have enabled cyberattacks and cyber exploitation efforts by state and non-state actors. While the technical details of how such attacks are conducted are not publicly available, it is highly probable that both the use of cryptanalysis and the absence of strong encryption were central to a number of cyberattacks with significant repercussions, ranging from the destruction of physical infrastructure to the theft of data critical to the security of citizens and the state.[181] The cybersecurity threat has been listed as a top global threat in the U.S. intelligence community's Worldwide Threat Assessment since 2013.[182]

Consequently, cryptography is relevant to national security on a number of fronts. It is often considered to be the only serious barrier to the conduct of signals intelligence—the stronger the cryptographic capabilities of the opponents, the more difficult it is to gather intelligence. This concern underpins the U.S. National Security Agency's (NSA) stance against the widespread deployment of strong cryptographic systems and the

---

[178] Rod J. Rosenstein, "Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy" (Annapolis, MD, October 10, 2017), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval.

[179] James A. Lewis, Denise E. Zheng, and William A. Carter, "The Effect of Encryption on Lawful Access to Communications and Data" (Center for Strategic and International Studies, February 8, 2017), https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data.

[180] Sean A. Morris, "The Misuse of Encryption and the Risks Posed to National Security" (Master's Capstone, Utica College, 2017), https://search.proquest.com/openview/dd0ee6680bb5d2171202152dbe433dd4/1.

[181] Herbert Lin, "Governance of Information Technology and Cyber Weapons," in *Governance of Dual-Use Technologies: Theory and Practice* (American Academy of Arts & Sciences, 2016), 112–57.

[182] National Academies of Sciences, Engineering, and Medicine, *Decrypting the Encryption Debate: A Framework for Decision Makers* (Washington, DC: The National Academies Press, 2018), https://doi.org/10.17226/25010.

adoption of strong cryptographic standards. Simultaneously, the NSA is heavily invested in strengthening the cryptographic technologies deployed for securing national infrastructure domestically.[183]

Tools Used to Control Cryptography R&D

Attempts to restrict research

Prior to the 1970s, cryptography was considered the domain of the U.S. government. The government was the exclusive owner of cryptography research, the primary employer of cryptography researchers, and the dominant user of cryptographic technologies. Their motivations for pursuing cryptography were twofold—to protect national secrets and to access information about their allies and adversaries deemed necessary for national security and foreign policy.

This began to change with the invention of public key cryptography in 1976 by Whitfield Diffie and Martin Hellman, two Stanford researchers.[184] Two years later, three researchers at the Massachusetts Institute of Technology (MIT)—Ronald Rivest, Adi Shamir, and Leonard Adleman—developed the first implementation of public key cryptography, which came to be known as the RSA algorithm.[185] The trio also invented digital signatures, enabling authentication as a fundamental component of the public key system. Public key cryptography could now be implemented as part of a commercial product for individuals and institutions, sitting squarely beyond the strict control of the USG.

As more researchers followed in the footsteps of Diffie, Hellman, and the RSA trio, the NSA began to try to limit the conduct and dissemination of public research on cryptography. The first target was the primary funder of public research on cryptography, the National Science Foundation (NSF). In 1977, the NSA approached Fred Weingarten, then Director of the Division of Computer Research at the NSF. Weingarten was told that federal law gave the NSA exclusive control over the conduct of cryptography research. When Weingarten challenged this claim, the NSA backed down and instead offered to review NSF grant proposals related to cryptography. The NSF agreed to this.[186] The NSA simultaneously began targeting researchers, particularly those on the brink of sharing their work publicly. In July 1977, NSA employee Joseph Meyer wrote to the Institute for Electrical and Electronics Engineers (IEEE) ahead of their planned October conference at Cornell University, the International Symposium on Information Theory, which was slated to feature a number of papers on encryption. The letter began by noting that "in the past months [...] various IEEE groups have been publishing and exporting technical articles on encryption and cryptology—a technical field which is covered by federal regulations." Meyer then proceeded to warn the IEEE that they would be in violation of the law should they allow these presentations to proceed: "I suggest that IEEE might want to review this situation, for these modern weapons technologies uncontrollably disseminated

[183] Susan Landau, "Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure," *Journal of National Security Law & Policy* 7, no. 3 (2014): 411, https://jnslp.com/2014/09/29/under-the-radar-nsas-efforts-to-secure-private-sector-telecommunications-infrastructure/.
[184] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory* 22, no. 6 (November 1976): 644–654, https://doi.org/10.1109/TIT.1976.1055638.
[185] Ronald Linn Rivest, Adi Shamir, and Leonard Max Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM* 21, no. 2 (February 1, 1978): 120–126, https://doi.org/10.1145/359340.359342.
[186] These efforts are particularly well documented in: Jenny Shearer and Peter Gutmann, "Government, Cryptography, and the Right to Privacy," *Journal of Universal Computer Science* 2, no. 3 (1996): 113–146, https://doi.org/10.3217/jucs-002-03-0113.

could have more than academic effect."[187] The conference organizers subsequently issued a letter to the academics scheduled to present at the conference to inform them of the situation. Nevertheless, the conference proceeded as planned. A number of universities explicitly supported their professors to present their research publicly despite the warnings, and when the NSA raised alarm at the posting of hard copies of the RSA algorithm paper globally, MIT's lawyers stepped in to successfully challenge this claim.[188]

In the early 1980s, the Reagan administration greatly bolstered the NSA's ability to restrict the publication of cryptography research. In April 1982, Executive Order 12356 eliminated the requirement that national security and public interest considerations had to be weighed before information could be classified.[189] In September 1984, NSDD-145 expanded the security classification system to encapsulate "sensitive but unclassified data."[190] As a result of both directives, the NSA became the primary gatekeeper for cryptography, telecommunications systems security, and information systems security issues. Specifically, the NSA was authorized to prescribe standards, methods, and procedures for restricting cryptographic material, techniques, and information in the name of national security.

However, the NSA increasingly showed signs of acknowledgement that restricting the dissemination of research was an increasingly futile effort. In 1980, Leonard Adleman—one of the inventors of the RSA algorithm—applied for a grant from the NSF which included some research on cryptography. Adleman reportedly received a call from the NSF stating that the NSA were insistent that they fund the portion of his grant on cryptography. Adleman was furious—"in my mind, this threatened the whole mission of the university and its place in society"—and was prepared to go public before NSA Director Inman himself called Adleman to apologize, claiming that this was a mistake. The NSA proceeded to allow the NSF to fund the entirety of Adleman's grant.[191]

Prepublication review

The only documented effort to establish a prepublication review system for cryptography research was initiated in 1979 by NSA Director Vice Admiral B.R. Inman, when he publicly voiced his concern that some information contained in published articles on cryptography endangered the mission of the NSA and thus U.S. national security.[192] [193] [194] The USG had become concerned that open publication of research

---

[187] Fred W. Weingarten, "Cryptography and National Security," *Information Systems Security* 1, no. 1 (1992): 9–12, https://doi.org/10.1080/19393559208551309.

[188] Kenneth J. Pierce, "Public Cryptography, Arms Export Controls, and the First Amendment: A Need for Legislation," *Cornell International Law Journal* 17, no. 1 (1984): 197, https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1136&context=cilj.

[189] The White House, "Executive Order 12356--National Security Information," 1982, https://www.archives.gov/federal-register/codification/executive-order/12356.html.

[190] The White House, "National Policy on Telecommunications and Automated Information Systems Security," National Security Decision Directive Number 145, September 17, 1984, https://fas.org/irp/offdocs/nsdd145.htm.

[191] Steven Levy, *Crypto: How the Code Rebels Beat the Government–Saving Privacy in the Digital Age* (East Rutherford: Penguin, 2001).

[192] Bobby R. Inman, "The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector," *Cryptologia* 3, no. 3 (1979): 129–135, https://doi.org/10.1080/0161-117991853954.

[193] Until then, the NSA did not have statutory power to require the submission of proposed publications for prior review or to require changes in publications prepared outside the agency and not under NSA contract or grant. However, the National Science Foundation announced during the process that it had responsibility under routine executive orders to refer cryptologic information developed in NSF-sponsored research projects that it believes may be classifiable to the NSA. See Jonathan Knight, "Cryptographic Research and NSA," *Academe* 67, no. 6 (1981): 371–82, https://doi.org/10.2307/40248881.

[194] In its current policy, the NSF states: "NSF grants are intended for unclassified, publicly releasable research. The grantee will not be granted access to classified information. NSF does not expect that the results of the research project

results in cryptography could reveal vulnerabilities in encryption algorithms that an enemy could exploit.[195] The cryptography research community argued, however, that in well-designed cryptographic systems, only the key needed to be secret and that general progress in the discipline would be best made under conditions of openness.[196] NSA Director Ingram proposed a dialogue with the academic community to satisfy the NSA's national security concerns about the publication of (non-governmental) cryptographic research papers without unduly hampering such research or impairing First Amendment rights. In response, the American Council on Education convened the Public Cryptography Study Group (PCSG) in 1980, consisting of selected academics working on cryptography as well as NSA staff. The PCSG first considered the introduction of a mandatory prepublication review procedure conducted by the NSA for all papers dealing with cryptography. The idea was rejected as the group members felt that they were not able to clearly evaluate the need for secrecy and that a voluntary agreement would gain them more support from the research community. Eventually, the PCSG recommended a system in which the NSA would invite authors to submit cryptography manuscripts for prior review at the same time that the manuscripts were submitted for publication. The NSA was to define the exact research areas covered by the system and manuscripts had to be returned promptly to the authors with explanations and recommendations in case of any national security concerns. With the support of all except one member, the PCSG accepted the proposal. However, neither the research community nor the NSA were entirely satisfied with the review system.

Despite the voluntary nature of the system, the research community criticized it before it was even introduced.[197] One member of the PCSG, the computer science and cryptography scholar George Davida, described the NSA's efforts as "unnecessary, divisive, wasteful and chilling."[198] He argued, for example, that the PCSG did not adequately consider the impact of restraints on research beyond the field of cryptography. Withholding basic research results in cryptography would negatively affect research not only within the discipline but also in adjacent disciplines including computer science and engineering. Davida further argued that such restraints would violate First Amendment rights and would only be the first step towards a mandatory system.[199]

The implementation of the review procedure, however, eased fears about impounded research and unnecessary constraints. There have been only a few requests from the NSA for prepublication review. In some cases, the NSA required minor changes. In a few instances, they asked scientists to hold back research results. In other cases, the NSA helped researchers to lift or avoid secrecy orders imposed on cryptography

---

will involve classified information. If, however, in conducting the activities supported under a grant , the PI/PD is concerned that any of the research results involve potentially classifiable information that may warrant Government restrictions on the dissemination of the results, the PI/PD should promptly notify the cognizant NSF Program Officer." See "Proposal and Award Policies and Procedures Guide" (National Science Foundation, January 30, 2017), 133, https://www.nsf.gov/pubs/policydocs/pappg17_1/nsf17_1.pdf.

[195] National Academy of Engineering, "Appendix E: Voluntary Restraints on Research with National Security Implications: The Case of Cryptography, 1975-1982," in *Scientific Communication and National Security* (Washington, DC: The National Academies Press, 1982), https://doi.org/10.17226/253.

[196] National Research Council (US) Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, "Information Restriction and Control Regimes," in *Biotechnology Research in an Age of Terrorism* (Washington, DC: National Academies Press (US), 2004), https://www.ncbi.nlm.nih.gov/books/NBK222057/.

[197] Jonathan Knight, "Cryptographic Research and NSA," *Academe* 67, no. 6 (1981): 371–82, https://doi.org/10.2307/40248881.; Davida, G. (1981).; George I. Davida, "The Case Against Restraints on Non-Governmental Research in Cryptography," *Cryptologia* 5, no. 3 (1981): 143–148, https://doi.org/10.1080/0161-118191855940.

[198] Davida, "The Case Against Restraints on Non-Governmental Research in Cryptography."

[199] Davida, "The Case Against Restraints on Non-Governmental Research in Cryptography."; Knight, "Cryptographic Research and NSA."

research under the Invention Secrecy Act (see below).[200] [201] From the perspective of the USG, the most significant problem was the possibility that a "blockbuster paper"—a paper reporting on research constituting a significant scientific breakthrough—might slip through the system and seriously damage U.S. national security.[202] However, over time, the government has been able to exercise some control over the publication of results through the introduction of the voluntary review system.

There is one notable case in which the NSA did demand that a paper be suppressed. Ralph Merkle, then a research scientist at Xerox PARC, had developed a set of algorithms that would significantly speed up cryptographic computation. In the same paper that described this breakthrough, Merkle also discussed in detail the inner workings of the Lucifer algorithm that underpinned the Data Encryption Standard (DES).[203] The NSA demanded that this paper be suppressed. Xerox, Merkle's employer at the time, complied. However, one of the reviewers of Merkle's paper, who objected to the NSA order, leaked a version of it on the Internet. The NSA consequently rescinded its request to withhold publication. Many perceived this as an acknowledgement that the ability for the NSA to restrict the publication of research was weakening in the face of a research community empowered by an open-source culture and the interconnectedness of the Internet.

Invention Secrecy Act

In 1978, the NSA drew on the Invention Secrecy Act of 1951 to attempt to block two patents from non-government cryptography researchers. The first was filed by Professor George Davida from the University of Wisconsin. When Davida went public about this, the university chancellor publicly denounced the NSA for obstructing academic freedom. The NSA subsequently rescinded the order.[204] The second was filed by freelance researcher Carl Nicolai. After an outcry in the media, this secrecy order was also rescinded.[205]

Export controls

Since the 1970s, the USG has also used export controls to limit the proliferation of encryption technology. The Arms Export Control Act (AECA) of 1976 authorized the DoD and other government agencies to regulate dual-use products, including encryption software and hardware. For those that did not classify as munition under the AECA, the Export Administration Act (EAA) of 1979 gave the Department of Commerce the ability to regulate encryption products. Export of strong encryption products thus required

---

[200] See section below on the "Invention Secrecy Act" for further information.
[201] Lance J. Hoffman, *Building in Big Brother: The Cryptographic Policy Debate* (New York: Springer, 1995).
[202] In August 1989, the computer scientists John Gilmore distributed a paper, written by Robert Merkle, describing fast and inexpensive ways of keeping computer information private over the objections of the NSA, see John Markoff, "Paper on Codes Is Sent Despite U.S. Objections," *The New York Times*, August 9, 1989, sec. U.S., https://www.nytimes.com/1989/08/09/us/paper-on-codes-is-sent-despite-us-objections.html.
[203] Ralph C. Merkle, "Fast Software Encryption Functions," in *Advances in Cryptology-CRYPTO' 90* (Conference on the Theory and Application of Cryptography, Santa Barbara, CA: Springer, 1990), 477–501, https://link.springer.com/content/pdf/10.1007/3-540-38424-3_34.pdf.
[204] Louis Kruh, "The Control of Public Cryptography and Freedom of Speech - a Review," *Cryptologia* 10, no. 1 (January 1, 1986): 2–9, https://doi.org/10.1080/0161-118691860741.; John Markoff, "A Public Battle Over Secret Codes," *The New York Times*, May 7, 1992, https://www.nytimes.com/1992/05/07/business/a-public-battle-over-secret-codes.html.
[205] Lee Ann Gilbert, "Patent Secrecy Orders: The Unconstitutionality of Interference in Civilian Cryptography Under Present Procedures," *Santa Clara Law Rev.* 22 (1982): 325, https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2035&context=lawreview.

explicit approval from the state; in practice, such exemptions were rarely granted.[206] This resulted in a two-tiered system of export-grade cryptography. Within the U.S., strong cryptography was permitted, whereas only cryptography of a substantially weaker grade could be exported abroad.[207] In practice, the NSA also used such controls to pressure manufacturers into weakening their products in the design phase.[208]

As private sector interests in cryptography increased during the 1990s, so did the industry's opposition to the export control regime. Studies cited losses in the scale of hundreds of millions of dollars in sales to foreign competitors. A landmark report from the National Research Council came down firmly against strict export control of cryptographic products. It concluded that not only did export control laws limit the ability for U.S. companies to retain market dominance, but they also reduced the domestic availability of strong encryption due to many U.S. vendors only investing resources into developing one export-grade product line.[209] Another National Research Council report warned that "if the U.S. does not allow vendors of commercial systems to export security products and products with relatively effective security features, large multinational firms as well as foreign consumers will simply purchase equivalent systems from foreign manufacturers."[210]

Members of Congress stirred into action in the early 1990s, most notably Representatives Maria Cantwell and Sam Gejdenson. In October 1993, Cantwell and Gejdenson held a subcommittee hearing to draw attention to the problem. Notably, testimony from Steve Walker, a former NSA official, referred to statistics that demonstrate how widespread cryptographic products were beyond U.S. borders: "The U.S. government is succeeding only in crippling a vital American industry's exporting ability."[211] Cantwell prepared the Legislation to Amend the Export Administration Act of 1979 in November 1993; if passed, the bill would substantially relax export regulations on public domain encryption software. Two days before the bill went to vote, then Vice President Al Gore wrote to Cantwell giving her forewarning that the administration was about to put forward a proposal for a key recovery system that would, in effect, achieve what her bill proposed. Cantwell subsequently dropped her bill.

Years later, the Clinton Administration took a number of steps to significantly relax export controls on encryption products. On September 16, 1998, Al Gore announced reforms to the export control regime that would allow U.S. companies to export encryption products to their overseas subsidiaries. The reforms also streamlined the licensing review process and brought the key-length requirements closer to marketplace realities for international encryption standards.[212] Both law enforcement officials and industry representatives expressed support for these reforms. In January 2000, the White House announced further substantive changes to the cryptographic export control regime that would provide U.S. companies much greater freedoms in exporting cryptographic products, specifically those intended for retail use. This marked

---

[206] Solveig Singleton, "Encryption Policy for the 21st Century: A Future without Government-Prescribed Key Recovery," Policy Analysis (Cato Institute, November 19, 1998), https://www.cato.org/publications/policy-analysis/encryption-policy-21st-century-future-without-governmentprescribed-key-recovery.
[207] Ben Buchanan, "Cryptography and Sovereignty," *Survival* 58, no. 5 (September 2016): 95–122, https://doi.org/10.1080/00396338.2016.1231534.
[208] David Banisar, "Stopping Science: The Case of Cryptography," *Health Matrix* 9, no. 2 (1999): 253, https://scholarlycommons.law.case.edu/healthmatrix/vol9/iss2/4/.
[209] National Research Council, *Cryptography's Role in Securing the Information Society*, ed. Kenneth W. Dam and Herbert S. Lin (Washington, DC: National Academies Press, 1996), https://doi.org/10.17226/5131.
[210] National Research Council, *Computers at Risk: Safe Computing in the Information Age* (Washington, DC: National Academies Press, 1991), https://doi.org/10.17226/1581.
[211] Levy, *Crypto*.
[212] Al Gore, "Holds News Briefing on Encryption" (The White House, September 16, 1998).

the end to a long battle over export controls—industry opposition ended, as did congressional attempts to modify the export control regime.[213]

Technical data related to cryptography was regulated by the same export control laws—specifically as deemed exports. Thus, the same regulatory uncertainty that plagued cryptography firms also applied to academic institutions and researchers producing this technical data. It was unclear, for example, whether it was illegal under the regime to discuss cryptography with a foreign citizen, teach courses on cryptography that involve non-U.S. graduate students, or allow foreign citizens residing in the U.S. to work on source code for cryptographic products.[214]

Two cases are often cited as examples of the export control regime restricting the actions of researchers. First was the case of Pretty Good Privacy (PGP), spearheaded by freelance software programmer Philip Zimmermann. PGP was released in 1991 as an open-source program used to encrypt mail messages end-to-end; a subsequent improved version of PGP was released in 1992. In 1993, Zimmermann became the target of a criminal investigation based on a possible violation of export control laws; the case was eventually dropped in 1996.[215]

The second was the case of Daniel Bernstein, who in 1995 had developed an encryption algorithm that he wished to publish and implement in the form of a computer program intended for distribution. He was prevented from doing so under export control laws and thus filed a suit against the government seeking to challenge their ability to bar the restriction of publications of cryptographic documents and software. Bernstein's case rested on the claim that the export control regime was an "impermissible prior restraint on speech, in violation of the First Amendment." At both the district court level and in the Appeals Court for the Ninth Circuit, Bernstein won. Judge Betty Fletcher from the Ninth Circuit court issued a landmark defense of cryptography as a vital component of democracy: "Government attempts to control encryption [...] may well implicate not only First Amendment rights of cryptographers, but also the constitutional rights of each of us as potential recipients of encryption's bounty."[216] The case was escalated to the Supreme Court but has since been indefinitely postponed.

At the multilateral scale, both the Coordinating Committee for Multilateral Export Controls (COCOM) and the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (WA) were light on regulating cryptographic technologies. In 1989, COCOM voted to decontrol password and authentication cryptographic products; in 1991, they decided to allow the export of mass market cryptographic software, including public domain software. The WA underwent a brief period of overt influence from the Clinton Administration in the 1990s and attempted to impose standardized restrictions on the export of encryption products that closely mirrored the U.S. export control laws at the time, but these restrictions did not last long.[217] In June 2000, the European Council of Ministers announced the end of cryptographic export controls within the European Union and with its trading and security

---

[213] Rebecca Christie, "U.S. Limbers up for Encryption Sales: Companies Are Cheered as Rules Are Eased on Exporting Privacy Software," *Financial Times (London)*, January 18, 2000.; T. E. Crocker, "Decoding Rules of Encryption: The Ins and Outs of New Regulations Governing Exports," *Legal Times*, 2000.; David E. Sanger and Jeri Clausing, "U.S. Removes More Limits On Encryption," *The New York Times*, January 13, 2000, https://www.nytimes.com/2000/01/13/business/us-removes-more-limits-on-encryption.html.

[214] National Research Council, *Cryptography's Role in Securing the Information Society*, ed. Kenneth W. Dam and Herbert S. Lin (Washington, DC: National Academies Press, 1996), https://doi.org/10.17226/5131.

[215] E. Cocoran, "U.S. Closes Investigation in Computer Privacy Case," *Washington Post*, 1996.

[216] Whitfield Diffie and Susan Landau, "The Export of Cryptography in the 20th Century and the 21st," April 19, 2005, https://privacyink.org/pdf/export_control.pdf.

[217] Aaron Pressman, "U.S. Claims Victory on Global Encryption Exports," *Reuters*, December 3, 1998.

partners, including the U.S. More recently, the European Union has called for the removal of cryptography from the WA altogether, stating: "Cryptography technology does not belong in the scope of dual-use export controls. It is the task of the [European] Commission to introduce coordinated activity of Member States in the framework of the Wassenaar Arrangement to eliminate cryptography technology from the list of controlled items."[218]

Intelligence collection and covert action

Edward Snowden's document leak revealed multiple strategies deployed by the NSA to subvert encryption across and beyond the U.S. The most prominent was a highly classified decryption program called Bullrun, the objective of which was to crack encryption of online communications and data, targeting widely used online protocols such as HTTPS, voice-over-IP, and Secure Sockets Layer (SSL).[219] The NSA appeared to utilize a number of methods, including computer network exploitation, industry relationships, and collaboration with foreign intelligence entities.[220]

In September 2013, it was further revealed that the NSA had strategically sought to undermine strong encryption by creating backdoors in numerous hardware and software products; instead of advocating publicly for key escrow, they had instead been engineering exceptional access surreptitiously.[221] Most notably, the NSA sought to compromise the Secure Hash Algorithm (SHA) standard. In 2007, NIST announced a competition to replace the hash standard SHA-1 whose weaknesses had become evident in recent years.[222] In 2012, they announced a winner to become SHA-3. Then in August 2013, NIST proposed an abbreviated version of the winning algorithm that would diminish the algorithm's robustness, to the consternation of industry and researchers alike.[223] The Snowden documents revealed that the NSA had been responsible. They had attempted to subvert the standard by proposing a weak random bit generator in the hash algorithm (NSA's random bit generator had been demonstrated to be vulnerable by two Microsoft researchers back in 2007[224]). *The New York Times* thus reported that the NSA had worked to "insert

---

[218] Amanda O'Keefe, "Why the EU's Call to Remove Crypto-Tech from Dual-Use Export Controls Is Encouraging," IAPP, January 3, 2018, https://iapp.org/news/a/why-the-eus-call-to-remove-crypto-tech-from-dual-use-export-controls-is-encouraging/.

[219] James Ball, Julian Borger, and Glenn Greenwald, "Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security," *The Guardian*, September 6, 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[220] Bert-Jaap Koops and Eleni Kosta, "Looking for Some Light through the Lens of 'Cryptowar' History: Policy Options for Law Enforcement Authorities against 'Going Dark,'" *Computer Law & Security Review* 34, no. 4 (August 2018): 890–900, https://doi.org/10.1016/j.clsr.2018.06.003.

[221] Sascha D. Meinrath and Sean Vitka, "Crypto War II," *Critical Studies in Media Communication* 31, no. 2 (June 2014): 123–28, https://doi.org/10.1080/15295036.2014.921320.; Tom Simonite, "NSA's Own Hardware Backdoors May Still Be a 'Problem from Hell,'" *MIT Technology Review*, October 8, 2013, https://www.technologyreview.com/2013/10/08/176195/nsas-own-hardware-backdoors-may-still-be-a-problem-from-hell/.

[222] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu, "Finding Collisions in the Full SHA-1," in *Advances in Cryptology – CRYPTO 2005* (25th Annual International Cryptology Conference, Santa Barbara, CA: Springer, 2005), 17–36, https://link.springer.com/chapter/10.1007/11535218_2.

[223] John Kelsey, "SHA3: Past, Present and Future" (Workshop on Cryptographic Hardware and Embedded Systems, Santa Barbara, CA, August 2013), https://csrc.nist.gov/CSRC/media/Projects/Hash-Functions/documents/kelsey_ches2013_presentation.pdf.

[224] Dan Shumow and Niels Ferguson, "On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng," http://rump2007.cr.yp.to/15-shumow.pdf.

vulnerabilities into commercial encryption systems" and "influence policies, standards and specifications for commercial public key technologies."[225]

[225] "Documents Reveal N.S.A. Campaign Against Encryption," *The New York Times*, September 5, 2013, https://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html.

Appendix B: Antitrust as a Strategic Lever

The Modern Antitrust Statutory Regime

This section details the statutory regimes relevant to the purposes of this paper.[226]

The Sherman Act

The Sherman Act is "the heart of [American] antitrust policy."[227] It contains two substantive provisions: Section 1[228] and Section 2.[229]

Section 1

"Section 1 of the Sherman Act prohibits agreements that unreasonably restrain trade."[230] It reads:

> Every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations, is declared to be illegal. Every person who shall make any contract or engage in any combination or conspiracy hereby declared to be illegal shall be deemed guilty of a felony . . . .[231]

It "applies to all sectors of the economy with limited exceptions . . . ."[232] "In determining whether a party has violated Section 1, courts determine first, whether there is an agreement, and second, whether the agreement is an unreasonable restraint of trade."[233]

Agreement

"An agreement for the purposes of US antitrust law need not be express, but can be tacit, signified with a wink and nod or handshake, or inferred from circumstantial evidence."[234] Courts will sometimes infer agreement from parallel business conduct when accompanied by "plus factors" such as motive to conspire, actions that only make sense in the context of an agreement, or contacts between competitors.[235]

---

[226] We did not include the Robinson–Patman Act, 15 U.S.C. §§ 13(a)–(f), which prevents exclusionary conduct by large *buyers*. *See* MacAvoy, *supra* note 136.
[227] *Id.*
[228] 15 U.S.C § 1.
[229] 15 U.S.C § 2.
[230] MacAvoy, *supra* note 136.
[231] 15 U.S.C. § 1.
[232] MacAvoy, *supra* note 136. Exemptions exist for certain labor union activities, agricultural cooperatives, export trade associations, state-regulated insurance, defense production arrangements under the Defense Production Act, charitable donations, newspaper joint operating arrangements, and state actions. *See id.*; *see generally Antitrust Affirmative Defenses: Overview*, Practical Law Practice Note 5-616-6893 (2018).
[233] MacAvoy, *supra* note 136.
[234] *Id.*
[235] *See id.*

Unreasonable Restraint of Trade

There are two tests for determining whether a restraint is unreasonable.[236] The first is the per se rule: certain restraints "are conclusively presumed to be unreasonable."[237] The idea behind this rule is that "certain kinds of agreements will so often prove so harmful to competition and so rarely prove justified that the antitrust laws do not require proof that an agreement of that kind is, in fact, anticompetitive in the particular circumstances."[238] Examples of per se restraints include price-fixing, bid-rigging, limits on output, and market division.[239] To prevail, a plaintiff must merely establish that a restraining agreement of this sort existed.[240]

Restraints to which the per se rule does not apply are analyzed under the "rule of reason."[241] The rule of reason weighs anticompetitive effects against procompetitive benefits. Under a rule-of-reason analysis, the plaintiff must prove that the challenged agreement substantially harms competition. Courts may "tak[e] into account a variety of factors, including specific information about the relevant business, its condition before and after the restraint was imposed, and the restraint's history, nature and effect."

Generally, courts will evaluate a defendant's market power in a properly defined relevant market to determine whether the agreement could harm competition. If, however, the plaintiff introduces persuasive evidence of actual detrimental effects (like reduced output) within the rough contours of a relevant market, that proof may obviate the need to prove market power in a relevant market. Rather, the evidence of anticompetitive effects may separately establish the defendant's market power.

Once the plaintiff demonstrates anticompetitive effects, the burden shifts to the defendant to show that its conduct served a legitimate business purpose and otherwise generated procompetitive benefits. The plaintiff then generally bears the ultimate burden to show that the anticompetitive effects outweigh any procompetitive benefits. The rule-of-reason test is fact-sensitive and more flexible than the per se rule.[242]

Section 2

Section 2 regulates monopolization.[243] It provides:

> Every person who shall monopolize, or attempt to monopolize, or combine or conspire with any other person or persons, to monopolize any part of the trade or commerce among the several States, or with foreign nations, shall be deemed guilty of a felony . . . .[244]

Note that "[m]onopolies by themselves are not unlawful under Section 2. Rather, what is unlawful is the exercise of monopoly power to exclude rivals and harm competition."[245] Thus, a Section 2 violation has two

---

[236] *See id.*
[237] *Id.*
[238] NYNEX Corp. v. Discon, Inc., 525 U.S. 128, 133 (1998).
[239] *See* MacAvoy, *supra* note 136.
[240] *See id.*
[241] *See id.*
[242] *Id.* (alteration in original) (citations omitted) (quoting State Oil Co. v. Khan, 522 U.S. 3, 10 (1997)).
[243] *See id.*
[244] 15 U.S.C. § 2.
[245] MacAvoy, *supra* note 136.

components: a large market share (i.e., monopoly) and exclusionary conduct in the acquisition or maintenance of that market share.[246]

Monopolization

Generally speaking, at least a 50% market share is necessary to be characterized as a monopoly for Section 2 purposes. A 70% share is usually sufficient, "at least when coupled with evidence of substantial barriers to entry."[247] "Market shares between 50% to 70% are generally viewed as in a gray area, and the outcome will be fact specific."[248] When determining whether a firm has a monopoly, courts will also consider barriers to market entry, the strength of competing firms, industry trends, customers' ease of switching suppliers, and the strength of demand.[249]

Unlawful Acquisition or Maintenance of Monopoly Power

Practices which could constitute exclusionary conduct (i.e., unlawful acquisition or maintenance of monopoly power) include predatory pricing,[250] disparagement of a competing product, frivolous lawsuits against competitors, refusals to deal, product bundling, and exclusive dealing.[251] Some business practices may be legal when practiced by non-monopolies, but illegal under Section 2 when practiced by monopolies.[252]

Clayton Act[253]

Among other things, the Clayton Act prohibits the following when they may "substantially lessen competition":

- price discrimination,
- exclusive dealing,
- conditioning supply of one product on agreement to buy another product, and
- mergers and acquisitions.[254]

Federal Trade Commission Act[255]

"The FTC [Federal Trade Commission] Act was designed to supplement and bolster the Sherman Act by enabling the FTC to stop in their incipiency practices which, when full blown, would violate the Sherman Act."[256] In addition to conduct that violates the Sherman Act, the FTC also uses the act to challenge:

---

[246] *See id.*
[247] *See id.*
[248] *Id.*
[249] *See id.*
[250] Predatory pricing requires (1) pricing below cost to drive out or discipline rivals, and (2) the ability to recoup losses from (1) through supracompetitive pricing. *See id.*
[251] *See id.*
[252] *See id.*
[253] 15 U.S.C. §§ 12–27.
[254] *See* MacAvoy, *supra* note 136.
[255] 15 U.S.C. §§ 41–58.
[256] MacAvoy, *supra* note 136.

1. Cases in which a firm invited a competitor to collude, but the competitor rejected the invitation.[257]

2. Cases in which a firm facilitates agreement, such as by exchanging competitive information, but in which there is no evidence of an agreement.[258]

State Laws

All U.S. states also have antitrust laws, which are enforceable independently of the federal laws.[259]

Enforcement Entities

The two primary enforcers of domestic antitrust law are the Department of Justice (DoJ) and the Federal Trade Commission (FTC).[260] "[Enforcement against v]arious industries [is] allocated to a particular agency, and the other agency agrees not to compete in investigating any antitrust matter involving that industry. For example, the oil industry 'belongs' to the FTC, and the steel industry 'belongs' to the DoJ."[261]

State Attorneys General

"State statutes empower state attorneys general to enforce their antitrust laws. As a company's anticompetitive conduct often affects both interstate and intrastate commerce, state attorneys general typically coordinate the investigation and prosecution of antitrust matters with other states and federal agencies."[262]

Private Individuals

Even if governmental actors choose not to prosecute antitrust violations, the antitrust laws enable harmed private individuals to seek compensation. Such private actions make up the overwhelming majority of antitrust enforcement.[263] They are therefore a potentially powerful deterrent, especially given the availability of class actions[264] and treble damages to successful plaintiffs.

---

[257] *See id.* Such conduct is not illegal under the Sherman Act because a rejected invitation to collude is not an "agreement."
[258] *See id.*
[259] *See id.*
[260] *See id.*
[261] William F. Shughart II, *Antitrust Policy in Virginia and Chicago*, Kan. J.L. & Pub. Pol'y, Winter 1995, at 27, 29.
[262] MacAvoy, *supra* note 136.
[263] *See* Steven C. Salop & Lawrence J. White, *Private Antitrust Litigation: Introduction and Framework*, *in* Private Antitrust Litigation: New Evidence, New Learning 3, 3–4 (Stephen C. Salop & Lawrence J. White eds., 1988); Amit Bindra, *Antitrust Class Action Litigation Post* Wal-Mart v. Dukes*: More of the Same*, 13 J. Bus. & Sec. L. 201, 210 (2013) ("[I]n the U.S., private action generates at least ninety percent of antitrust enforcement.").
[264] *See Antitrust Class Certification*, Practical Law Practice Note w-009-9818 (2018).

Consequences

Criminal Penalties

Violation of Section 1[265] of the Sherman Act is a felony.[266] The maximum punishments per violation are $100 million for corporations and $1 million for individuals.[267] Individuals can face up to ten years in prison in addition to fines.[268] Only the DoJ can prosecute criminal antitrust charges.[269]

Civil Damages

All antitrust statutes allow for civil damages.[270] Violations of the Sherman Act, the Clayton Act, and some state antitrust laws carry treble damages, including for private plaintiffs.[271] The FTC Act also provides for civil penalties.[272]

Equitable[273] Relief

Equitable remedies available under the Sherman and Clayton Acts include "[i]njunctive orders to prevent and restrain violations of the antitrust laws" and "[s]tructural remedies (including dissolution and divestiture) in order to restore competition."[274]

Equitable remedies available under the FTC Act include "[c]ease and desist orders" and disgorgement.[275]

State antitrust laws allow for injunctive relief.[276]

Merger Review

When reviewing mergers, the enforcement agencies can condition mergers on restructuring to preserve competition (especially through divestiture of specific assets),[277] fair dealing, mandatory licensing, contracting prohibitions, anti-retaliation agreements, internal firewalls, and transparency measures.[278]

---

[265] In principle, Section 2 can carry criminal sanctions as well, but "the DOJ does not generally prosecute violations of Section 2 criminally." *See* MacAvoy, *supra* note 136.
[266] *See id.*
[267] *See id.*
[268] *See id.*
[269] *See id.*
[270] *See id.*
[271] *See id.*
[272] *See id.*
[273] "When a court awards a nonmonetary judgment, such as an order to do something (mandamus or specific performance) or refrain from doing something (injunction), when monetary damages are not sufficient to repair the injury." *Equitable Relief*, Wex, https://www.law.cornell.edu/wex/equitable_relief (last visited June 13, 2018).
[274] MacAvoy, *supra* note 136.
[275] "A remedy requiring a party who profits from illegal or wrongful acts to give up any profits he or she made as a result of his or her illegal or wrongful conduct. The purpose of this remedy is to prevent unjust enrichment." *Disgorgement*, Wex, https://www.law.cornell.edu/wex/disgorgement (last visited June 13, 2018).
[276] *See* MacAvoy, *supra* note 136.
[277] Structural remedies can also include licensing and asset swaps. *See* Laura A. Wilkinson & Alexis Brown-Reilly, *Merger Remedies*, Practical Law Practice Note 6-521-6515 (2018).
[278] *See id.*

Consent Decrees[279]

An antitrust agency may enter into a consent decree with a defendant to avoid further litigation. FTC consent decrees are publicly posted for comments and subject to approval by the commission.[280] "DOJ consent decrees are subject to the Tunney Act, which requires that a federal district court review the proposed remedy and the competitive impact of the proposed decree in the relevant markets. The Tunney Act also requires a 60-day public notice and comment period before the judge issues a final order."[281] "[O]ne of the motivations for enacting the Tunney Act was to shield antitrust decisions from politics."[282]

[279] "A court order to which all parties have agreed. It is often done after a settlement between the parties that is subject to approval by the court." *Consent Decree*, WEX, https://www.law.cornell.edu/wex/consent_decree (last visited June 13, 2018).
[280] *See* Wilkinson & Brown-Reilly, *supra* note 273.
[281] *Id.* (citation omitted) (citing 15 U.S.C. § 16).
[282] Robert W. Hahn & Anne Layne-Farrar, *Federalism in Antitrust*, 26 HARV. J.L. & PUB. POL'Y 877, 894 (2003).

Appendix C: The "Born Secret Doctrine"—Public Backlash

When the "Born Secret Doctrine" was introduced, journalists and researchers criticized it as "a potent suppressor of free speech" and as incompatible with the U.S. Constitution's First Amendment.[283] Prior restraint, referring to prior censorship of information or prepublication censorship (which also applies to the Invention Secrecy Act) has been called "the most serious and least tolerable" restrictions on the First Amendment by some legal scholars,[284] although the Supreme Court never held that these practices were unconstitutional.

The tension between free speech and prior restraint with regard to the Born Secret Doctrine was illustrated in a landmark case, *United States v. Progressive, Inc.* (1979). The Department of Energy filed a lawsuit against The Progressive, a monthly journal, over the publication of an article on the H-bomb. The Department of Energy claimed that the article, written by Howard Morland, revealed the design of the Teller-Ulam H-bomb, and therefore fell under the "born secret" clause, although Morland claimed that all information that the article was based on came from publicly available sources. The Department of Energy dropped the case and declared it "moot" after other information related to the article's content were published independently. Hence, the legality of the doctrine has never been truly challenged in court.[285]

Today, resistance against the "born secret doctrine" has notably diminished. This, however, seems particular to the case of nuclear weapons-related research. A substantial consensus developed after the Second World War among scientists and the public that secrecy in the case of nuclear weapons is justified and should be maintained. The emerging taboo against nuclear weapons use[286] and the recognition of the dangers associated with nuclear weapon proliferation to non-state actors probably contributed to this shift.[287] However, other restrictions concerning the broader field of nuclear science, such as restricted access for students from certain countries to study nuclear science, remain contested.

---

[283] Howard Morland, "Born Secret," *Cardozo Law Review* 26, no. 4 (2005): 1401–8, https://fas.org/sgp/eprint/cardozo.pdf. See also Paul N. McCloskey, "'Born Secret' Disclosure Law," *Physics Today* 33, no. 7 (1980): 9–13, https://doi.org/10.1063/1.2914200.

[284] Jonathan L Entin, "United States v. Progressive, Inc.: The Faustian Bargain and the First Amendment," *Northwestern University Law Review* 75, no. 1 (1978): 538–69, footnote 2, https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1466&context=faculty_publications.

[285] For a detailed overview of the case, see Alexander DeVolpi et al., Born Secret: The H-Bomb, the Progressive Case and National Security (New York: Pergamon Press, 1981).

[286] Nina Tannenwald, "The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use," *International Organization* 53, no. 3 (1999): 433–468, https://doi.org/10.1162/002081899550959.

[287] National Research Council (US) Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, "Information Restriction and Control Regimes," in *Biotechnology Research in an Age of Terrorism* (Washington, DC: National Academies Press (US), 2004), https://www.ncbi.nlm.nih.gov/books/NBK222057/.

Bibliography

Aftergood, Steven. "Invention Secrecy Statistics." Federation of American Scientists Project on Government Secrecy, 2020. https://fas.org/sgp/othergov/invention/stats.html.

Alic, John A, Lewis M. Branscomb, Harvey Brooks, Ashton B. Carter, and Gerald L. Epstein. *Beyond Spinoff: Military and Commercial Technologies in a Changing World*. Boston, Mass.: Harvard Business School Press, 1992.

Alothman, Khalid, Terri L. Gabriel, Kevin F. Hanrahan, Jeffrey Howell, Benjamin Lam, Steven Mapes, Adrian Meyer, et al. "Spring 2017 Industry Study: Electronics." The Dwight D. Eisenhower School for National Security and Resource Strategy, National Defense University, 2017. https://es.ndu.edu/Portals/75/Documents/industry-study/reports/2017/es-is-report-electronics-2017.pdf.

Alper, Alexandra. "U.S. Government Limits Exports of Artificial Intelligence Software." *Reuters*, January 3, 2020. https://www.reuters.com/article/usa-artificial-intelligence-idUSL1N2980M0.

Andrews, Edmund L. "Cold War Secrecy Still Shrouds Inventions." *The New York Times*, May 23, 1992. https://www.nytimes.com/1992/05/23/business/patents-cold-war-secrecy-still-shrouds-inventions.html.

Armstrong, Martin. "Infographic: The Companies With the Most AI Patents." *Statista Infographics*, May 29, 2019. https://www.statista.com/chart/18211/companies-with-the-most-ai-patents/.

Arnold, Zachary, Roxanne Heston, Remco Zwetsloot, and Tina Huang. "Immigration Policy and the U.S. AI Sector." Center for Security and Emerging Technology, September 2019. https://cset.georgetown.edu/wp-content/uploads/CSET_Immigration_Policy_and_AI.pdf.

Baldwin, Kristen. "DoD Electronics Priorities." NDIA Electronics Division, January 18, 2018. https://www.ndia.org/-/media/sites/ndia/divisions/electronics/past-proceedings/ndia-ed-baldwin-18jan2018-vf.ashx?la=en.

Ball, James, Julian Borger, and Glenn Greenwald. "Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security." *The Guardian*, September 6, 2013. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

Banisar, David. "Stopping Science: The Case of Cryptography." *Health Matrix* 9, no. 2 (1999): 253. https://scholarlycommons.law.case.edu/healthmatrix/vol9/iss2/4/.

Beahn, John M., Robert S. Larussa, and Lisa Raisner. "Final CFIUS Regulations Implement Significant Changes by Broadening Jurisdiction and Updating Scope of Reviews." Shearman & Sterling, January 14, 2020. https://www.shearman.com/perspectives/2020/01/final-cfius-regulations-implement-changes-by-broadening-jurisdiction-and-updating-scope-of-reviews.

Berge, Wendell. *Cartels: Challenge to a Free World*. Washington, DC: Public Affairs Press, 1944.

Bergen, Mark, Sarah Frier, and Selina Wang. "Google, Facebook, Twitter Scramble to Hold Washington at Bay." *Bloomberg*, October 10, 2017. https://www.bloomberg.com/news/articles/2017-10-10/google-facebook-and-twitter-scramble-to-hold-washington-at-bay.

Borkin, Joseph. *The Crime and Punishment of IG Farben*. New York: The Free Press, 1978.

Brown, Clair, and Greg Linden. *Chips and Change: How Crisis Reshapes the Semiconductor Industry*. Cambridge: MIT Press, 2011.

Brown, Michael, and Pavneet Singh. "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation." Defense Innovation Unit Experimental, January 2018. https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf.

Brustein, Joshua. "Congratulations, Your Genius Patent Is Now a Military Secret." *Bloomberg*, June 8, 2016.

https://www.bloomberg.com/news/articles/2016-06-08/congratulations-your-genius-patent-is-now-a-military-secret.
Buchanan, Ben. "Cryptography and Sovereignty." *Survival* 58, no. 5 (September 2016): 95–122. https://doi.org/10.1080/00396338.2016.1231534.
Bureau of Industry and Security. "2016 Report on Foreign Policy-Based Export Controls," 2016. https://www.bis.doc.gov/index.php/documents/public-policy/1396-bis-foreign-policy-report-2016/file.
———. "CCL: Country Group 1," February 24, 2020. https://www.bis.doc.gov/index.php/documents/regulation-docs/452-supplement-no-1-to-part-740-country-groups/file.
———. "Commerce Control List: Category 3 - Electronics," May 23, 2019. https://www.bis.doc.gov/index.php/documents/regulations-docs/2334-ccl3-8/file.
———. "Commerce Control List (CCL)." Accessed June 19, 2020. https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl.
———. "Entity List," 2019. https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list.
———. "Guidance to the Commerce Department's Reexport Controls," 2011. https://www.bis.doc.gov/index.php/documents/licensing-forms/4-guidelines-to-reexport-publications/file.
———. "Identification and Review of Controls for Certain Foundational Technologies." *Federal Register* 85, no. 167 (August 27, 2020): 52934–35. https://www.federalregister.gov/documents/2020/08/27/2020-18910/identification-and-review-of-controls-for-certain-foundational-technologies.
———. "Review of Controls for Certain Emerging Technologies." *Federal Register* 83, no. 223 (November 19, 2018): 58201–2. https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies.
———. "Revisions to the Export Administration Regulations (EAR)." *Federal Register* 77, no. 72 (April 13, 2012): 22191–200. https://www.govinfo.gov/content/pkg/FR-2012-04-13/pdf/2012-8944.pdf.
Castellanos, Sara. "AI, Quantum R&D Funding to Remain a Priority Under Biden." *Wall Street Journal*, November 9, 2020. https://www.wsj.com/articles/ai-quantum-r-d-funding-to-remain-a-priority-under-biden-11604944800.
———. "Executives Say $1 Billion for AI Research Isn't Enough." *Wall Street Journal*, September 10, 2019. https://www.wsj.com/articles/executives-say-1-billion-for-ai-research-isnt-enough-11568153863.
Cecire, Michael H, and Heidi M Peters. "The Defense Production Act (DPA) and COVID-19: Key Authorities and Policy Considerations." Congressional Research Service, March 18, 2020. https://fas.org/sgp/crs/natsec/IN11231.pdf.
Center for Energy Economics. "Export Regulations: What You Need To Know," 2013. https://web.archive.org/web/20160822035527/http://www.beg.utexas.edu/energyecon/CEE_Exploring%20Export%20Controls.pdf.
Center for Nuclear Studies, K=1 Project. "Stuxnet: Tool of Nonproliferation or Pandora's Box," August 19, 2012. https://k1project.columbia.edu/news/stuxnet.
Chen, Eric B. "Technology Outpacing the Law: The Invention Secrecy Act of 1951 and the Outsourcing of US Patent Application Drafting." *Texas Intellectual Property Law Journal* 13 (2004): 352–75. http://www.tiplj.org/wp-content/uploads/Volumes/v13/v13p351.pdf.
Christie, Rebecca. "U.S. Limbers up for Encryption Sales: Companies Are Cheered as Rules Are Eased on Exporting Privacy Software." *Financial Times (London)*, January 18, 2000.
Cocoran, E. "U.S. Closes Investigation in Computer Privacy Case." *Washington Post*, 1996.

Coleman, Mary Sue. "Balancing Science and Security." *Science* 365, no. 6449 (July 12, 2019): 101–101. https://doi.org/10.1126/science.aay5856.
Council, National Research. *Computers at Risk: Safe Computing in the Information Age*. Washington, DC: National Academies Press, 1991. https://doi.org/10.17226/1581.
———. *Cryptography's Role in Securing the Information Society*. Edited by Kenneth W. Dam and Herbert S. Lin. Washington, DC: National Academies Press, 1996. https://doi.org/10.17226/5131.
Crocker, T. E. "Decoding Rules of Encryption: The Ins and Outs of New Regulations Governing Exports." *Legal Times*, 2000.
Cummings, Mary L. "Artificial Intelligence and the Future of Warfare." Chatham House, January 2017. https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings.pdf.
Dafoe, Allan. "AI Governance: A Research Agenda." Oxford, UK: Governance of AI Program, Future of Humanity Institute, University of Oxford, 2018. https://www.fhi.ox.ac.uk/wp-content/uploads/GovAI-Agenda.pdf.
Daley, Jason. "Milestone Carbon-Nanotube Microchip Sends First Message: 'Hello World!'" *Smithsonian Magazine*, August 29, 2019. https://www.smithsonianmag.com/smart-news/advanced-carbon-nanotube-microprocessor-created-180973013/.
"Damnjanovic v. U.S. Air Force," 2015. https://fas.org/sgp/othergov/invention/damn-complaint.pdf.
DARPA. "DARPA Electronics Resurgence Initiative," April 2, 2020. https://www.darpa.mil/work-with-us/electronics-resurgence-initiative.
———. "Designing Chips for Real Time Machine Learning," March 21, 2019. https://www.darpa.mil/news-events/2019-03-21.
Davida, George I. "The Case Against Restraints on Non-Governmental Research in Cryptography." *Cryptologia* 5, no. 3 (1981): 143–148. https://doi.org/10.1080/0161-118191855940.
Davis, Bob, Kate O'Keeffe, and Asa Fitch. "Taiwan Firm to Build Chip Factory in U.S." *Wall Street Journal*, May 15, 2020. https://www.wsj.com/articles/taiwan-company-to-build-advanced-semiconductor-factory-in-arizona-11589481659.
Dentons. "New CFIUS Rules under FIRRMA: What Foreign Investors and US Businesses Need to Know," January 24, 2020. https://www.dentons.com/en/insights/alerts/2020/january/24/new-cfius-rules-under-firrma-what-foreign-investors-and-us-businesses-need-to-know.
Department of Justice. "Applied Materials Inc. and Tokyo Electron Ltd. Abandon Merger Plans After Justice Department Rejected Their Proposed Remedy," April 27, 2015. https://www.justice.gov/opa/pr/applied-materials-inc-and-tokyo-electron-ltd-abandon-merger-plans-after-justice-department.
———. "Three South Korean Companies Agree to Plead Guilty and to Enter into Civil Settlements for Rigging Bids on United States Department of Defense Fuel Supply Contracts." Press Release, November 14, 2018. https://perma.cc/7922-UU28.
DeVolpi, Alexander, Gerald E. Marsh, Ted A. Postol, and George S. Stanford. *Born Secret: The H-Bomb, the Progressive Case and National Security*. New York: Pergamon Press, 1981.
Diffie, Whitfield, and Martin Hellman. "New Directions in Cryptography." *IEEE Transactions on Information Theory* 22, no. 6 (November 1976): 644–654. https://doi.org/10.1109/TIT.1976.1055638.
Diffie, Whitfield, and Susan Landau. "The Export of Cryptography in the 20th Century and the 21st," April 19, 2005. https://privacyink.org/pdf/export_control.pdf.
Ding, Jeffrey, and Allan Dafoe. "The Logic of Strategic Assets: From Oil to Artificial Intelligence," January 9, 2020. http://arxiv.org/abs/2001.03246.

Directorate for Financial and Enterprise Affairs. "Public Interest Considerations in Merger Control: Note by the United States," June 2, 2016. https://perma.cc/XB26-CRTP.
Donovan, Jim. *Shoot for the Moon: The Space Race and the Extraordinary Voyage of Apollo 11*. New York: Little, Brown and Company, 2019.
Edwards, Corwin D. "Thurman Arnold and the Antitrust Laws." *Political Science Quarterly* 58, no. 3 (1943): 338–355.
Entin, Jonathan L. "United States v. Progressive, Inc.: The Faustian Bargain and the First Amendment." *Northwestern University Law Review* 75, no. 1 (1978): 538–69. https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1466&context=faculty_publications.
Facebook. "Facebook Inc. ANPRM Comments," January 10, 2019. https://www.regulations.gov/document?D=BIS-2018-0024-0212.
Fantl, Jeremy. "Knowledge How." In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta. Metaphysics Research Lab, Stanford University, 2017. https://plato.stanford.edu/archives/fall2017/entries/knowledge-how/.
Farnam, Julie. *US Immigration Laws under the Threat of Terrorism*. Algora Publishing, 2005.
Federal Trade Commission. "Broadcom Limited/Brocade Communications Systems, In the Matter Of," July 12, 2017. https://www.ftc.gov/enforcement/cases-proceedings/171-0027/broadcom-limitedbrocade-communications-systems.
———. "Intel Corporation, In the Matter Of," November 2, 2010. https://www.ftc.gov/enforcement/cases-proceedings/061-0247/intel-corporation-matter.
———. "Qualcomm Inc.," November 25, 2019. https://www.ftc.gov/enforcement/cases-proceedings/141-0199/qualcomm-inc.
Federation of American Scientists Project on Government Secrecy. "Invention Secrecy Statistics," 2019. https://fas.org/sgp/othergov/invention/stats.html.
Feng, Emily. "Visas Are The Newest Weapon In U.S.-China Rivalry." *NPR*, April 25, 2019. https://www.npr.org/2019/04/25/716032871/visas-are-the-newest-weapon-in-u-s-china-rivalry.
Fiegerman, Seth, and Jackie Wattles. "Trump Stops China-Backed Takeover of U.S. Chip Maker." *CNN Money*, September 14, 2017. https://money.cnn.com/2017/09/13/technology/business/trump-lattice-china/index.html.
Fisher, Thomas K. "Antitrust during National Emergencies: I." *Michigan Law Review* 40, no. 7 (1942): 969–1004.
———. "Antitrust during National Emergencies: II." *Michigan Law Review* 40, no. 8 (1942): 1161–1199.
Fitch, Asa, Kate O'Keeffe, and Bob Davis. "Trump and Chip Makers Including Intel Seek Semiconductor Self-Sufficiency." *Wall Street Journal*, May 11, 2020. https://www.wsj.com/articles/trump-and-chip-makers-including-intel-seek-semiconductor-self-sufficiency-11589103002.
Flynn, Carrick. "Recommendations on Export Controls for Artificial Intelligence." Center for Security and Emerging Technology, February 2020. https://cset.georgetown.edu/wp-content/uploads/Recommendations-on-Export-Controls-for-Artificial-Intelligence.pdf.
Foster, Dakota, and Zachary Arnold. "Antitrust and Artificial Intelligence: How Breaking Up Big Tech Could Affect the Pentagon's Access to AI." Center for Security and Emerging Technology, 2020. https://doi.org/10.51593/20190025.
Fung, Brian, and Hamza Shaban. "Want to Understand How Dominant Tech Companies Have Become? Look at the Number of Issues They Lobby On." *Washington Post*, August 31, 2017. https://www.washingtonpost.com/news/the-switch/wp/2017/08/31/want-to-understand-how-dominant-tech-companies-have-become-look-at-the-number-of-issues-they-lobby-on/.

Gafni, Jonathan, Thomas A McGrath, and January Kim. "Mandatory CFIUS Filings Under the Final FIRRMA Regulations." Linklaters, January 28, 2020. https://www.linklaters.com/en/insights/publications/us-publications/2020/january/mandatory-cfius-filings-under-the-final-firrma-regulations.

Gates, Bill. "We're Defending Our Right to Innovate." *Wall Street Journal*, May 20, 1998. https://www.wsj.com/articles/SB895616628927103500.

Gibson Dunn. "New Controls on Emerging Technologies Released, While U.S. Commerce Department Comes Under Fire for Delay", October 27, 2020. https://www.gibsondunn.com/new-controls-on-emerging-technologies-released-while-us-commerce-department-comes-under-fire-for-delay/#_ftn1

Gilbert, Lee Ann. "Patent Secrecy Orders: The Unconstitutionality of Interference in Civilian Cryptography Under Present Procedures." *Santa Clara Law Rev.* 22 (1982): 325. https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2035&context=lawreview.

Gimbel, John. "Project Paperclip: German Scientists, American Policy, and the Cold War." *Diplomatic History* 14, no. 3 (1990): 343–65. https://www.jstor.org/stable/24911848.

Goel, Vindu. "How Trump's 'Hire American' Order May Affect Tech Worker Visas." *The New York Times*, April 18, 2017. https://www.nytimes.com/2017/04/18/technology/h1b-visa-facts-tech-worker.html.

Goodfellow, Ian. "I Emphatically Agree. My Collaborators' Visa Restrictions Have Been One of the Largest Bottlenecks to Our Collective Research Productivity over the Last Few Years." Twitter, February 13, 2019. https://twitter.com/goodfellow_ian/status/1095727254057840640.

Goodman, Matthew P., and David A. Parker. "The China Challenge and CFIUS Reform." *CSIS Global Economics Monthly*, March 31, 2017. https://www.csis.org/analysis/global-economics-monthly-china-challenge-and-cfius-reform.

Google. "Google Comment - ANPRM - Review of Controls for Certain Emerging Technologies," January 10, 2019. https://www.regulations.gov/document?D=BIS-2018-0024-0160.

Gore, Al. "Holds News Briefing on Encryption." The White House, September 16, 1998.

Graham, Thomas, and Keith A. Hansen. *Preventing Catastrophe: The Use and Misuse of Intelligence in Efforts to Halt the Proliferation of Weapons of Mass Destruction*. Stanford: Stanford University Press, 2009.

Greyber, Howard D., Robert L. Park, and Brandee L. Telford. "Supercomputer Access." *Physics Today* 39, no. 12 (1986): 15. https://doi.org/10.1063/1.2815234.

Griffin, Patrick. "CFIUS in the Age of Chinese Investment." *Fordham Law Review* 85, no. 4 (2017): 1757–92. https://ir.lawnet.fordham.edu/flr/vol85/iss4/9.

Gronvall, Gigi Kwik. "H5N1: A Case Study for Dual-Use Research." Council on Foreign Relations, 2013. https://www.centerforhealthsecurity.org/our-work/publications/h5n1-a-case-study-for-dual-use-research.

Hahn, Robert W., and Anne Layne-Farrar. "Federalism in Antitrust." *Harvard Journal of Law and Public Policy* 26 (2003): 877,894.

Hanemann, Thilo, Cassie Gao, and Adam Lysenko. "Net Negative: Chinese Investment in the US in 2018." Rhodium Group, January 13, 2019. https://rhg.com/research/chinese-investment-in-the-us-2018-recap/.

Harper, Jon. "Pentagon Struggling to Attract Artificial Intelligence Experts." *National Defense*, July 14, 2017. https://www.nationaldefensemagazine.org/articles/2017/7/14/pentagon-in-artificial-intelligence-arms-race-with-commercial-industry.

Heaven, Will Douglas. "The White House Wants to Spend Hundreds of Millions More on AI Research." *MIT Technology Review*, February 11, 2020. https://www.technologyreview.com/2020/02/11/844891/the-white-house-will-spend-hundreds-of-millions-more-on-ai-research/.

Hempel, Jessi. "DOD Head Ashton Carter Enlists Silicon Valley to Transform the Military." *Wired*, November 18, 2015. https://www.wired.com/2015/11/secretary-of-defense-ashton-carter/.
Hewlett, Richard G. "A Historian's View." *Bulletin of the Atomic Scientists* 37, no. 10 (1981): 20–27. 10.1080/00963402.1981.11458919.
Hoffman, Lance J. *Building in Big Brother: The Cryptographic Policy Debate*. New York: Springer, 1995.
Horan, Donald. "National Defense Executive Reserve Program." U.S. General Accounting Office. Accessed June 18, 2020. https://www.gao.gov/assets/210/206264.pdf.
House Subcommittee on Antitrust, Commercial and Administrative Law. "Investigation of Competition in Digital Markets: Majority Staff Report and Recommendations," 2020. https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf.
Huang, Tina, and Zachary Arnold. "Immigration Policy and the Global Competition for AI Talent." Center for Security and Emerging Technology, 2020. https://cset.georgetown.edu/research/immigration-policy-and-the-global-competition-for-ai-talent/.
Hunt, Linda. *Secret Agenda: The United States Government, Nazi Scientists, and Project Paperclip, 1945 to 1990*. New York: St. Martin's Press, 1991.
Hunt, Will, and Remco Zwetsloot. "The Chipmakers: U.S. Strengths and Priorities in the High-End Semiconductor Workforce." Center for Security and Emerging Technology, 2020. https://cset.georgetown.edu/research/the-chipmakers-u-s-strengths-and-priorities-for-the-high-end-semiconductor-workforce.
Hunter, Andrew P, and Lindsey R Sheppard. "Artificial Intelligence and National Security: The Importance of the AI Ecosystem." Center for Strategic and International Studies, November 5, 2018. https://www.csis.org/analysis/artificial-intelligence-and-national-security-importance-ai-ecosystem.
Inman, Bobby R. "The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector." *Cryptologia* 3, no. 3 (1979): 129–135. https://doi.org/10.1080/0161-117991853954.
Irfan, Muhammad. "US May Block Chinese Investment in Artificial Intelligence in Silicon Valley." *Daily Pakistan Global*, June 14, 2017. https://en.dailypakistan.com.pk/technology/us-may-block-chinese-investment-in-artificial-intelligence-in-silicon-valley/.
Jackson, James K. "The Committee on Foreign Investment in the United States (CFIUS)." Congressional Research Service, February 14, 2020. https://fas.org/sgp/crs/natsec/RL33388.pdf.
Jing, Meng. "China Must Woo Top Tech Talent Turned off by Trump, Says Baidu Chief." *CNBC / South China Morning Post*, March 6, 2017. https://www.cnbc.com/2017/03/06/china-must-woo-top-tech-talent-turned-off-by-trump-says-baidu-chief.html.
Kang, C. S. Eliot. "U.S. Politics and Greater Regulation of Inward Foreign Direct Investment." *International Organization* 51, no. 2 (1997): 301–33. https://doi.org/10.1162/002081897550375.
Kania, Elsa B. "Beyond CFIUS: The Strategic Challenge of China's Rise in Artificial Intelligence." *Lawfare*, June 20, 2017. https://www.lawfareblog.com/beyond-cfius-strategic-challenge-chinas-rise-artificial-intelligence.
Kearney, James K., and Womble Carlyle. "Export Control Regulations and Participation by Foreign Nationals in University Research." Washington, DC, 2004. https://doi.org/10.4135/9781412969024.n90.
Kelley, Michael B., and Geoffrey Ingersoll. "The U.S. Started A Worldwide Cyberwar." *Business Insider*, October 18, 2012. https://www.businessinsider.com/us-started-worldwide-cyberwar-hacking-2012-10?r=US&IR=T#ixzz2IKHj4cee.

Kelsey, John. "SHA3: Past, Present and Future." Presented at the Workshop on Cryptographic Hardware and Embedded Systems, Santa Barbara, CA, August 2013. https://csrc.nist.gov/CSRC/media/Projects/Hash-Functions/documents/kelsey_ches2013_presentation.pdf.

Khula, Bruce A. "Antitrust at the Water's Edge: National Security and Antitrust Enforcement." *Notre Dame Law Review* 78 (2003): 629.

Kluckhohn, Frank L. "Arnold Says Standard Oil Gave Nazis Rubber Process." *The New York Times*, March 27, 1942. https://www.nytimes.com/1942/03/27/archives/arnold-says-standard-oil-gave-nazis-rubber-process-says-standard.html.

Knight, Jonathan. "Cryptographic Research and NSA." *Academe* 67, no. 6 (1981): 371–82. https://doi.org/10.2307/40248881.

Koops, Bert-Jaap, and Eleni Kosta. "Looking for Some Light through the Lens of 'Cryptowar' History: Policy Options for Law Enforcement Authorities against 'Going Dark.'" *Computer Law & Security Review* 34, no. 4 (August 2018): 890–900. https://doi.org/10.1016/j.clsr.2018.06.003.

Kruh, Louis. "The Control of Public Cryptography and Freedom of Speech - a Review." *Cryptologia* 10, no. 1 (January 1, 1986): 2–9. https://doi.org/10.1080/0161-118691860741.

Landau, Susan. "Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure." *Journal of National Security Law & Policy* 7, no. 3 (2014): 411. https://jnslp.com/2014/09/29/under-the-radar-nsas-efforts-to-secure-private-sector-telecommunications-infrastructure/.

Lapedus, Mark. "A Crisis In DoD's Trusted Foundry Program?" *Semiconductor Engineering*, October 22, 2018. https://semiengineering.com/a-crisis-in-dods-trusted-foundry-program.

Levy, Steven. *Crypto: How the Code Rebels Beat the Government–Saving Privacy in the Digital Age*. East Rutherford: Penguin, 2001.

Lewis, James A., Denise E. Zheng, and William A. Carter. "The Effect of Encryption on Lawful Access to Communications and Data." Center for Strategic and International Studies, February 8, 2017. https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data.

Liling, Qiu. "中國企業開出2至3倍薪資挖角 台灣已流失3000多名半導體業人才." *CMMedia*, December 3, 2019. https://www.cmmedia.com.tw/home/articles/18815.

Lin, Herbert. "Governance of Information Technology and Cyber Weapons." In *Governance of Dual-Use Technologies: Theory and Practice*, 112–57. American Academy of Arts & Sciences, 2016.

Lineback, Rob. "Semiconductor R&D Spending Will Step Up After Slowing." *IC Insights*, January 31, 2019. https://www.icinsights.com/news/bulletins/Semiconductor-RD-Spending-Will-Step-Up-After-Slowing/.

Lunden, Ingrid. "US Patents Hit Record 333,530 Granted in 2019; IBM, Samsung (Not the FAANGs) Lead the Pack." *TechCrunch*, January 14, 2020. https://social.techcrunch.com/2020/01/14/us-patents-hit-record-333530-granted-in-2019-ibm-samsung-not-the-faangs-lead-the-pack/.

MacAvoy, Christopher J. "US Antitrust Laws: Overview." Practice Note 9-204-0472. Practical Law, 2018.

Makinson, Larry. "Outsourcing the Pentagon." The Center for Public Integrity, September 29, 2004. https://publicintegrity.org/national-security/outsourcing-the-pentagon/.

Maldonado, Samantha. "Employees of Big Tech Are Speaking out like Never Before." *AP News*, August 25, 2019. https://apnews.com/80c76d32c7de48269cbd7bb9f838834c.

Markoff, John. "A Public Battle Over Secret Codes." *The New York Times*, May 7, 1992. https://www.nytimes.com/1992/05/07/business/a-public-battle-over-secret-codes.html.

———. "Paper on Codes Is Sent Despite U.S. Objections." *The New York Times*, August 9, 1989. https://www.nytimes.com/1989/08/09/us/paper-on-codes-is-sent-despite-us-objections.html.

Markoff John, and Rosenberg Matthew. "China Gains on the U.S. in the Artificial Intelligence Arms Race." *New York Times (China Edition)*, February 4, 2017. https://cn.nytimes.com/world/20170204/artificial-intelligence-china-united-states/en-us/.
McCabe, John. "Biden Vows Immigration Reform to Attract Top Talent to the US." *Science|Business*, January 21, 2021. https://sciencebusiness.net/news/biden-vows-immigration-reform-attract-top-talent-us.
McCloskey, Paul N. "'Born Secret' Disclosure Law." *Physics Today* 33, no. 7 (1980): 9–13. https://doi.org/10.1063/1.2914200.
McLaughlin, David. "Trump Blocks Broadcom Takeover of Qualcomm on Security Risks." *Bloomberg*, March 12, 2018. https://www.bloomberg.com/news/articles/2018-03-12/trump-issues-order-to-block-broadcom-s-takeover-of-qualcomm-jeoszwnt.
McLeary, Paul. "Pentagon To Classify More Acquisition Info, Keep Closer Eye On Fed Employees." *Breaking Defense*, October 2, 2019. https://breakingdefense.com/2019/10/pentagon-to-classify-more-acquisition-info-keep-closer-eye-on-fed-employees/.
Meinrath, Sascha D., and Sean Vitka. "Crypto War II." *Critical Studies in Media Communication* 31, no. 2 (June 2014): 123–28. https://doi.org/10.1080/15295036.2014.921320.
Merkle, Ralph C. "Fast Software Encryption Functions." In *Advances in Cryptology-CRYPTO' 90*, 477–501. Santa Barbara, CA: Springer, 1990. https://link.springer.com/content/pdf/10.1007/3-540-38424-3_34.pdf.
Mervis, Jeffrey. "Elite Advisers to Help NSF Navigate Security Concerns." *Science* 363, no. 6433 (March 22, 2019): 1261–1261. https://doi.org/10.1126/science.363.6433.1261.
Mitchell, Graham R. "The Global Context for U.S. Technology Policy." Washington, DC: U.S. Dept. of Commerce, Office of Technology Policy, 1997. https://permanent.fdlp.gov/lps12230/nas.pdf.
Moore, Samuel K. "DARPA'S $1.5-Billion Remake of U.S. Electronics: Progress Report." *IEEE Spectrum*, June 27, 2019. https://spectrum.ieee.org/tech-talk/semiconductors/devices/darpas-15billion-remake-of-us-electronics-progress-report.
Morland, Howard. "Born Secret." *Cardozo Law Review* 26, no. 4 (2005): 1401–8. https://fas.org/sgp/eprint/cardozo.pdf.
Morris, Sean A. "The Misuse of Encryption and the Risks Posed to National Security." Master's Capstone, Utica College, 2017. https://search.proquest.com/openview/dd0ee6680bb5d2171202152dbe433dd4/1.
Mourning, H.L., J.C. Morris, and Bret Convey. "Patent Security Category Review List." Armed Services Patent Advisory Board, January 1971. https://fas.org/sgp/othergov/invention/pscrl.pdf.
Mozur, Paul. "Obama Moves to Block Chinese Acquisition of a German Chip Maker." *The New York Times*, December 2, 2016. https://www.nytimes.com/2016/12/02/business/dealbook/china-aixtron-obama-cfius.html.
Mozur, Paul, and Jane Perlez. "China Bets on Sensitive U.S. Start-Ups, Worrying the Pentagon." *The New York Times*, March 22, 2017. https://www.nytimes.com/2017/03/22/technology/china-defense-start-ups.html.
National Academies of Sciences, Engineering, and Medicine. *Decrypting the Encryption Debate: A Framework for Decision Makers*. Washington, DC: The National Academies Press, 2018. https://doi.org/10.17226/25010.
National Academy of Engineering. "Appendix E: Voluntary Restraints on Research with National Security Implications: The Case of Cryptography, 1975-1982." In *Scientific Communication and National Security*. Washington, DC: The National Academies Press, 1982. https://doi.org/10.17226/253.

National Institutes of Health (NIH). "Press Statement on the NSABB Review of H5N1 Research," September 18, 2015. https://www.nih.gov/news-events/news-releases/press-statement-nsabb-review-h5n1-research.
National Research Council (US) Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology. "Information Restriction and Control Regimes." In *Biotechnology Research in an Age of Terrorism*. Washington, DC: National Academies Press (US), 2004. https://www.ncbi.nlm.nih.gov/books/NBK222057/.
National Science Foundation. "Funding and Support Descriptions." Accessed June 15, 2020. https://www.nsf.gov/homepagefundingandsupport.jsp.
———. "Proposal & Award Policies & Procedures Guide (Chapter VII - Grant Administration)." Accessed June 15, 2020. https://www.nsf.gov/pubs/policydocs/pappg20_1/pappg_7.jsp.
———. "Proposal and Award Policies and Procedures Guide," January 30, 2017. https://www.nsf.gov/pubs/policydocs/pappg17_1/nsf17_1.pdf.
National Security Commission on Artificial Intelligence. "First Quarter Recommendations," March 2020. https://drive.google.com/file/d/1wkPh8Gb5drBrKBg6OhGu5oNaTEERbKss/view.
National Security Commission on Artificial Intelligence. "Final Report," March 2021. https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.
National Soc. of Professional Engineers v. United States, 435 US. No. 76-1767 (Supreme Court 1978).
NBC Bay Area. "Schmidt on Antitrust: Competition Is One Click Away." *NBC Bay Area*, September 21, 2011. https://www.nbcbayarea.com/news/national-international/schmidt-on-antitrust-competition-is-one-click-away/1901637/.
New America. "Open Markets Applauds the European Commission's Finding Against Google for Abuse of Dominance," June 27, 2017. http://newamerica.org/open-markets/press-releases/open-markets-applauds-european-commissions-finding-against-google-abuse-dominance/.
Nynex Corp. v. Discon, Inc., 525 US. No. 96-1570 (Supreme Court 1998).
OECD. "Main Science and Technology Indicators," 2018. https://stats.oecd.org/Index.aspx?DataSetCode=MSTI_PUB#.
———. "Measuring Distortions in International Markets: The Semiconductor Value Chain." OECD Trade Policy Papers. OECD, December 12, 2019. https://www.oecd-ilibrary.org/trade/measuring-distortions-in-international-markets_8fe4491d-en.
O'Keefe, Amanda. "Why the EU's Call to Remove Crypto-Tech from Dual-Use Export Controls Is Encouraging." IAPP, January 3, 2018. https://iapp.org/news/a/why-the-eus-call-to-remove-crypto-tech-from-dual-use-export-controls-is-encouraging/.
O'Keefe, Cullen. "How Will National Security Considerations Affect Antitrust Decisions in AI? An Examination of Historical Precedents." Future of Humanity Institute, University of Oxford, 2020. https://www.fhi.ox.ac.uk/antitrust-okeefe.
OpenAI. "OpenAI Response Regarding ANPRM Controls for Certain Emerging Technologies," January 10, 2019. https://www.regulations.gov/document?D=BIS-2018-0024-0195.
Pierce, Kenneth J. "Public Cryptography, Arms Export Controls, and the First Amendment: A Need for Legislation." *Cornell International Law Journal* 17, no. 1 (1984): 197. https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1136&context=cilj.
Pitofsky, Robert. "Antitrust Modified: Education, Defense, and Other Worthy Enterprises." *Antitrust* 9 (Spring 1995): 23.
Practical Law. "Antitrust Affirmative Defenses: Overview." Practice Note 5-616-6893. Practical Law, 2018.
———. "Antitrust Class Certification." Practice Note w-009-9818. Practical Law, 2018.
Pressman, Aaron. "U.S. Claims Victory on Global Encryption Exports." *Reuters*, December 3, 1998.

Qualcomm. "Qualcomm Announces Fourth Quarter and Fiscal 2019 Results," November 6, 2019. https://www.qualcomm.com/news/releases/2019/11/06/qualcomm-announces-fourth-quarter-and-fiscal-2019-results.

Rabe, Stephen G. *Eisenhower and Latin America: The Foreign Policy of Anticommunism*. Chapel Hill, NC: UNC Press, 1988.

Rhyne, Darren. "DoD to Cancel Military Critical Technology List Instruction." Defense Acquisition University, December 19, 2018. https://www.dau.edu/cop/stm/blog/Lists/Posts/Post.aspx?List=d622f3dd%2D00cc%2D4c80%2D9238%2D9da31c0433a0&ID=21&Web=c7d4d9c5%2D6f41%2D468f%2Dad9f%2D714c2bf89c04.

Rill, James F., and Stacy L. Turner. "Presidents Practicing Antitrust: Where to Draw the Line." *Antitrust LJ* 79, no. 2 (2014): 577. https://www.jstor.org/stable/43486917.

Rivest, Ronald Linn, Adi Shamir, and Leonard Max Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." *Communications of the ACM* 21, no. 2 (February 1, 1978): 120–126. https://doi.org/10.1145/359340.359342.

Roane, Kit R. "A Scientific Thaw During the Cold War." Pulitzer Center, May 2, 2016. https://pulitzercenter.org/reporting/scientific-thaw-during-cold-war.

Rosenstein, Rod J. "Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy." Annapolis, MD, October 10, 2017. https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval.

Roumeliotis, Greg. "U.S. Blocks Chip Equipment Maker Xcerra's Sale to Chinese State Fund." *Reuters*, February 23, 2018. https://www.reuters.com/article/us-xcerra-m-a-hubeixinyan-idUSKCN1G703H.

Roumeliotis, Greg, and Diane Bartz. "U.S. Toughens Stance on Foreign Deals in Blow to China's Buying Spree." *Reuters*, July 20, 2017. https://www.reuters.com/article/us-usa-china-companies-idUSKBN1A532M.

Salop, Steven C., and Lawrence J. White. "Private Antitrust Litigation: An Introduction and Framework." In *Private Antitrust Litigation: New Evidence, New Learning*, edited by Steven C. Salop and Lawrence J. White, Vol. 3. Massachusetts Institute of Technology Press Cambridge, MA, 1988.

Sanger, David E. "U.S. to Restrict Supercomputer Use by Soviet Scholars." *The New York Times*, February 10, 1986. https://www.nytimes.com/1986/02/10/us/us-to-restrict-supercomputer-use-by-soviet-scholars.html.

Sanger, David E., and Jeri Clausing. "U.S. Removes More Limits On Encryption." *The New York Times*, January 13, 2000. https://www.nytimes.com/2000/01/13/business/us-removes-more-limits-on-encryption.html.

Sargent Jr., John F. "Federal Research and Development (R&D) Funding: FY2020." Congressional Research Service, March 18, 2020. https://fas.org/sgp/crs/misc/R45715.pdf.

Sargent Jr., John F., Marcy E Gallo, and Moshe Schwartz. "The Global Research and Development Landscape and Implications for the Department of Defense." Washington, DC: Congressional Research Service, November 8, 2018. https://fas.org/sgp/crs/natsec/R45403.pdf.

Schlager, Ivan A., Daniel J. Gerkin, Anthony Rapa, Lucille Hague, Mario Mancuso, Nathan L. Mitchell, Sanjay José Mullick, and Michelle A. Weinbaum. "CFIUS Goes Back to the Future by Tying Mandatory Filings Pertaining to Critical Technologies to U.S. Export Controls Assessments." Kirkland & Ellis, October 21, 2020. https://www.kirkland.com/publications/kirkland-alert/2020/10/cfius-critical-technologies.

Schulz, G.W. "Government Secrecy Orders on Patents Have Stifled More Than 5,000 Inventions." *Wired*, April 16, 2013. https://www.wired.com/2013/04/gov-secrecy-orders-on-patents/.

Semiconductor Industry Association. “2019 Factbook,” May 2019. https://www.semiconductors.org/wp-content/uploads/2019/05/2019-SIA-Factbook-FINAL.pdf.
———. “SIA Workforce Roundtable Summary Report,” March 16, 2018. https://www.semiconductors.org/wp-content/uploads/2018/06/Roundtable_Summary_Report_-_FINAL.pdf.
———. “Winning the Future: A Blueprint for Sustained U.S. Leadership in Semiconductor Technology,” April 2019. https://www.semiconductors.org/wp-content/uploads/2019/04/FINAL-SIA-Blueprint-for-web.pdf.
Shane, Scott, and Daisuke Wakabayashi. “‘The Business of War’: Google Employees Protest Work for the Pentagon.” *The New York Times*, April 4, 2018. https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html.
Sharp, Gregg S. “A Layman’s Guide to Intellectual Property in Defense Contracts.” *Public Contract Law Journal* 33, no. 1 (2003): 99–137. https://www.jstor.org/stable/25755261.
Shearer, Jenny, and Peter Gutmann. “Government, Cryptography, and the Right to Privacy.” *Journal of Universal Computer Science* 2, no. 3 (1996): 113–146. https://doi.org/10.3217/jucs-002-03-0113.
Sheehan, Matt. “Who Loses from Restricting Chinese Student Visas?” MacroPolo, May 31, 2018. https://macropolo.org/who-loses-from-restricting-chinese-student-visas/.
Shughart, William F. “Antitrust Policy in Virginia and Chicago.” *Kansas Journal of Law and Public Policy* 4 (1994): 27.
Shumow, Dan, and Niels Ferguson. “On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng.” 2007. http://rump2007.cr.yp.to/15-shumow.pdf.
Simonite, Tom. “NSA’s Own Hardware Backdoors May Still Be a ‘Problem from Hell.’” *MIT Technology Review*, October 8, 2013. https://www.technologyreview.com/2013/10/08/176195/nsas-own-hardware-backdoors-may-still-be-a-problem-from-hell/.
Singleton, Solveig. “Encryption Policy for the 21st Century: A Future without Government-Prescribed Key Recovery.” Policy Analysis. Cato Institute, November 19, 1998. https://www.cato.org/publications/policy-analysis/encryption-policy-21st-century-future-without-governmentprescribed-key-recovery.
Somerville, Heather. “Chinese Tech Investors Flee Silicon Valley as Trump Tightens Scrutiny.” *Reuters*, January 7, 2019. https://www.reuters.com/article/us-venture-china-regulation-insight-idUSKCN1P10CB.
Stacey, Kiran. “US Pledges to Limit Export Controls on Advanced Tech.” *Financial Times*, February 28, 2019. https://www.ft.com/content/ab4313dc-3b7d-11e9-b72b-2c7f526ca5d0.
State Oil Co. v. Khan, 522 US. No. 96-871 (Supreme Court 1997).
Steurer, Richard M., and Peter A. Barile III. “Antitrust in Wartime.” *Antitrust* 16 (Spring 2002): 71.
Stewart, Emily. “Facebook’s Latest Reason It Shouldn’t Be Broken up: Chinese Companies Will Dominate.” *Vox*, May 20, 2019. https://www.vox.com/recode/2019/5/20/18632669/sheryl-sandberg-break-up-facebook-china-cnbc.
Stocking, George Ward, and Myron M. Watkins. *Cartels in Action - Case Studies in International Business Diplomacy.* New York: Twentieth Century Fund, 1946.
Stone, I.F. “Thurman Arnold and the Railroads.” *The Nation*, March 6, 1943.
Strumpf, Dan. “U.S. Sets Export Controls on China’s Top Chip Maker.” *Wall Street Journal*, September 28, 2020. https://www.wsj.com/articles/u-s-sets-export-controls-on-chinas-top-chip-maker-11601118353.
Stucke, Maurice E. “Reconsidering Antitrust’s Goals.” *Boston College Law Review* 53 (2012): 551, 556, 563–66. https://lawdigitalcommons.bc.edu/bclr/vol53/iss2/4/.

Swayne, Matt. "The World's Top 12 Quantum Computing Research Universities." *The Quantum Daily*, November 18, 2019. https://thequantumdaily.com/2019/11/18/the-worlds-top-12-quantum-computing-research-universities/.

Tannenwald, Nina. "The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use." *International Organization* 53, no. 3 (1999): 433–468. https://doi.org/10.1162/002081899550959.

Taplin, Jonathan. "Why Is Google Spending Record Sums on Lobbying Washington?" *The Guardian*, July 30, 2017. https://www.theguardian.com/technology/2017/jul/30/google-silicon-valley-corporate-lobbying-washington-dc-politics.

Teece, D.J., Pisano, G. and Shuen, A., "Dynamic capabilities and strategic management," Strat. Mgmt. J., no. 18 (1997): 509-533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z

The New York Times. "A Top Chinese Scientist Was Deported by U.S." *The New York Times*, October 17, 1964. https://www.nytimes.com/1964/10/17/archives/a-top-chinese-scientist-was-deported-by-us-dr-tsien-may-have-a-role.html.

———. "Documents Reveal N.S.A. Campaign Against Encryption." *The New York Times*, September 5, 2013. https://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html.

The Wassenaar Arrangement. "About Us," 2020. https://www.wassenaar.org/about-us/.

The White House. "Executive Order 11858--Foreign Investment in the United States," May 7, 1975. https://www.archives.gov/federal-register/codification/executive-order/11858.html.

———. "Executive Order 12356--National Security Information," 1982. https://www.archives.gov/federal-register/codification/executive-order/12356.html.

———. "National Policy on Telecommunications and Automated Information Systems Security." National Security Decision Directive Number 145, September 17, 1984. https://fas.org/irp/offdocs/nsdd145.htm.

———. "NSDD-189: National Policy on the Transfer of Scientific, Technical and Engineering Information," 1985. https://www.aau.edu/key-issues/nsdd-189-white-house-1985-directive-fundamental-research-exemption.

———. "Proclamation on the Suspension of Entry as Nonimmigrants of Certain Students and Researchers from the People's Republic of China," May 29, 2020. https://web.archive.org/web/20210116212117/https://www.whitehouse.gov/presidential-actions/proclamation-suspension-entry-nonimmigrants-certain-students-researchers-peoples-republic-china/.

Thomsen II, Roszel C. "Artificial Intelligence and Export Controls: Conceivable, but Counterproductive?" *Journal of Internet Law* 12, no. 5 (November 2018). https://t-b.com/wp-content/uploads/2019/01/AI-and-Export-Controls-Journal-of-Internet-Law-Article.pdf.

TOP500. "TOP500 Supercomputer Sites," November 2019. https://www.top500.org/lists/2019/11/.

Tucker, Patrick. "What's the 'Risk' in China's Investments in US Artificial Intelligence? New Bill Aims to Find Out." *Defense One*, June 22, 2017. https://www.defenseone.com/technology/2017/06/how-not-win-ai-arms-race-china/138919/.

United States v. American Tel. and Tel. Co., 552 F. Supp. 131, 149, 149 n.77. Civ. A. No. 74-1698 (D.D.C. 1982).

U.S. Congress. Immigration and Nationality Act, 1182 8 USC § 212. Accessed June 16, 2020. https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title8-section1182&num=0&edition=prelim.
———. National Science Foundation Act of 1950 (1950). https://www.nsf.gov/about/history/legislation.pdf.
———. Penalty, 35 U.S. Code § 186 (2011). https://www.law.cornell.edu/uscode/text/35/186.
———. Right to compensation, 35 U.S. Code § 183 (2011). https://www.law.cornell.edu/uscode/text/35/183.
———. Rules and Regulations, Delegation of Power, 35 U.S. Code § 188 (1952). https://www.law.cornell.edu/uscode/text/35/188.
———. "S.Amdt.2244 to S.Amdt.2301 to S.4049," July 21, 2020. https://www.congress.gov/amendment/116th-congress/senate-amendment/2244/text.
———. Secrecy of certain inventions and withholding of patent, 35 U.S. Code § 181 (1952). https://www.law.cornell.edu/uscode/text/35/181.
———. The Foreign Risk Review Modernization Act of 2018 (2018). https://home.treasury.gov/sites/default/files/2018-08/The-Foreign-Investment-Risk-Review-Modernization-Act-of-2018-FIRRMA_0.pdf.
U.S. Department of Commerce, Bureau of Export Administration. "Critical Technology Assessment of the U.S. Artificial Intelligence Sector," August 1994. https://www.bis.doc.gov/index.php/documents/technology-evaluation/33-critical-technology-assessment-of-u-s-artificial-intelligence-1994/file.
U.S. Department of State. "Technology Alert List," August 2002. https://www.bu.edu/isso/files/pdf/tal.pdf.
U.S. Department of the Treasury. "The Committee on Foreign Investment in the United States (CFIUS)," 2021. https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius.
Vanian, Jonathan. "Apple Just Got More Public About Its Artificial Intelligence Plans." *Fortune*, July 19, 2017. https://fortune.com/2017/07/19/apple-artificial-intelligence-research-journal/.
Vogel, Kenneth P. "Google Critic Ousted From Think Tank Funded by the Tech Giant." *The New York Times*, August 30, 2017. https://www.nytimes.com/2017/08/30/us/politics/eric-schmidt-google-new-america.html.
———. "New America, a Google-Funded Think Tank, Faces Backlash for Firing a Google Critic." *The New York Times*, September 1, 2017. https://www.nytimes.com/2017/09/01/us/politics/anne-marie-slaughter-new-america-google.html.
Waller, Spencer Weber. "The Antitrust Legacy of Thurman Arnold." *St. John's Law Review* 78 (2004): 569.
Wang, Xiaoyun, Yiqun Lisa Yin, and Hongbo Yu. "Finding Collisions in the Full SHA-1." In *Advances in Cryptology – CRYPTO 2005*, 17–36. Santa Barbara, CA: Springer, 2005. https://link.springer.com/chapter/10.1007/11535218_2.
Warren, Elizabeth. "Here's How We Can Break up Big Tech," October 11, 2019. https://medium.com/@teamwarren/heres-how-we-can-break-up-big-tech-9ad9e0da324c.
Weingarten, Fred W. "Cryptography and National Security." *Information Systems Security* 1, no. 1 (1992): 9–12. https://doi.org/10.1080/19393559208551309.
Wex. "Consent Decree." Accessed June 13, 2018. https://www.law.cornell.edu/wex/consent_decree.
———. "Equitable Relief." Accessed June 13, 2018. https://www.law.cornell.edu/wex/equitable_relief.
Wilkinson, Laura A., and Alexis Brown-Reilly. "Merger Remedies." Practice Note 6-521-6515. Practical Law, 2018.

Williams, Robert Chadwell, and Philip Louis Cantelon. *The American Atom: A Documentary History of Nuclear Policies from the Discovery of Fission to the Present, 1939-1984*. Philadelphia: University of Pennsylvania Press, 1984.

Wilson, Christine S. "Welfare Standards Underlying Antitrust Enforcement: What You Measure Is What You Get." Arlington, VA: Federal Trade Commission, February 15, 2019. https://www.ftc.gov/system/files/documents/public_statements/1455663/welfare_standard_speech_-_cmr-wilson.pdf.

Work, Bob. "Remarks by Deputy Secretary Work on Third Offset Strategy." Brussels, Belgium, April 28, 2016. https://www.defense.gov/Newsroom/Speeches/Speech/Article/753482/remarks-by-deputy-secretary-work-on-third-offset-strategy/.

Yue, Pan. "China May Own More Artificial Intelligence Patents Than US By Year-End." *China Money Network*, September 14, 2017. https://www.chinamoneynetwork.com/2017/09/14/china-may-hold-artificial-intelligence-patents-us-year-end.

Zwetsloot, Remco, James Dunham, Zachary Arnold, and Tina Huang. "Keeping Top AI Talent in the United States." Center for Security and Emerging Technology, December 2019. https://cset.georgetown.edu/wp-content/uploads/Keeping-Top-AI-Talent-in-the-United-States.pdf.

Zwetsloot, Remco, Roxanne Heston, and Zachary Arnold. "Strengthening the U.S. AI Workforce." Center for Security and Emerging Technology, September 2019. https://cset.georgetown.edu/wp-content/uploads/CSET_U.S._AI_Workforce.pdf.

Zwetsloot, Remco, Baobao Zhang, Markus Anderljung, Michael C. Horowitz, and Allan Dafoe. "The Immigration Preferences of Top AI Researchers: New Survey Evidence." Perry World House and The Future of Humanity Institute, 2021. https://global.upenn.edu/perryworldhouse/news/immigration-preferences-top-ai-researchers-new-survey-evidence.