BLOCK-CHAIN REACTION: CORPORATE CONSIDERATIONS FOR COMPLIANCE WITH EXPORT CONTROLS AND REGULATIONS

TYLER GODBEHERE*

CONTENTS

I. INTRODUCTION

Assume that Pied Piper, a small startup technology company headquartered in Silicon Valley, hires a prominent Chinese engineer from Intel in 2018. This employee will work at the California office and assist Pied Piper in creating a new Internet that will revolutionize the technology industry. The company believes that the new engineer's expertise in semiconductor manufacturing equipment ("SME") will allow the team to finally complete this project. Once completed, Pied Piper plans to take the new Internet to the market where the product will compete with both U.S. and foreign competitors. This type of advanced technology is classified as "dual-use"[1] by the federal government and accordingly is subject to export controls and regulations ("Export Controls"). Since the new employee is a Chinese National, Pied Piper must obtain a *deemed export* license for this engineer to work with the emerging technology—regardless of the fact that this

* J.D., Class of 2020, Arizona State University Sandra Day O'Connor College of Law.

[1] *See* 15 C.F.R. § 730.3 (2020) (referring to the catchall designation of technology deemed to have both civil and military applications under the Export Administration Regulations).

engineer is already located in the United States or if the employee has a legal work visa.[2] Prior to 2018, when the engineer was working at Intel, the licensing requirement was never an issue because licenses were routinely granted after a one-month period.

In 2018, the Trump Administration began implementing a protectionist foreign policy. Under this new policy, the approval process for deemed export licenses transitioned from regularly being granted to a presumption of denial. This protectionist approach aligns with the federal government's philosophy to "ensure that U.S and allied country firms retain a dominant position in the global semiconductor market."[3] This assumes that companies, including startups like Pied Piper, have the compliance resources in place to comply with Export Controls. This policy leaves companies with two options: first, not hire or fire the foreign employee or alternatively, transfer the employee to a different position that does not involve regulated technology and therefore will not require a license. In either situation Piped Pier must replace the engineer, ideally with a U.S. citizen, to work on the regulated Internet—assuming such a qualified person exists in the job market.[4]

Technological advancements, amid the Sino-American Trade War, are delayed because of Export Controls. Companies are reluctant to hire foreign employees subject to Export Controls, regardless of whether they are the most qualified job candidates. Generally, employers are prohibited from discriminating against any employee because of the individual's nationality or race under both Title VII of the Civil Rights Act of 1964[5] and the Immigration Reform and Control Act of 1986.[6] Yet, distinctions based on citizenship are often synonymous with the protected classes of nationality or race.[7] However, these classifications appear to be permissible under exceptions to federal anti-discrimination laws regarding BFOQs,[8] national security requirements,[9] or general compliance with other U.S. laws.[10] At this time, it is unclear whether an exception to the

---

[2] *See* 15 C.F.R. § 734.13(a)(2) (2020) (deeming any transfer of the information regarding the regulated technology as a direct export to China).

[3] NAT'L SEC. COMM'N ON ARTIFICIAL INTELLIGENCE, INTERIM REPORT (Nov. 2019), https://epic.org/foia/epic-v-ai-commission/AI-Commission-Interim-Report-Nov-2019.pdf.

[4] Alison D. Raymore, *CIO Jury: 83% of CIOs Struggle to Find Tech Talent*, TECHREPUBLIC (June 16, 2017), https://www.techrepublic.com/article/cio-jury-83-of-cios-struggle-to-find-tech-talent/; Elizabeth L. LaRocca & Erin N. Bass, *Export Control Hiring Practices Continue to Challenge Employers*, STEPTOE (Nov. 1, 2018), https://www.lexology.com/library/detail.aspx?g=ec27f5b2-f6e4-430d-8fed-9f28a9c7b982.

[5] 42 U.S.C.A. § 2000e-2(a) (West 2020) (prohibiting employers from discriminating employees because of national origin or race, among other protected classes and specifying that it is unlawful for employers to practice employment practices that adversely affect or deprive employees of work opportunities based on national origin or race).

[6] 8 U.S.C.A. § 1324b(a)(1) (West 2020) (prohibiting employers from discriminating employees because of their national origin).

[7] LaRocca & Bass, *supra* note 4; *see generally* 8 U.S.C.A. § 1324.

[8] *See* 42 U.S.C.A. § 2000e-2(e) (West 2020) (stating that employers may lawfully make employment decisions because of national origin in circumstances when such a classification is a "bona fide occupational qualification reasonably necessary to the normal operation of that particular business or enterprise").

[9] *See* 42 U.S.C.A. § 2000e-2(g) (West 2020) (allowing employers to lawfully consider an individual's national origin in making employment decisions — such as hiring or firing an employee — when the performance of the job is subject to any national security requirement imposed by the United States and the individual has not satisfied that requirement).

[10] *See* 8 U.S.C.A. § 1324b(a)(2) (West 2020) (stating that employers can consider citizenship status where a citizenship requirement is necessary to comply with any Federal, State, or local law, or when the citizenship

anti-discrimination statutes would apply to a license requirement based purely on economic policy—rather than national security concerns. However, more importantly, it remains unknown whether the current deemed export requirement is constitutional under an Equal Protection Analysis.

Despite potential constitutional issues with Export Controls, companies seeking to operate in the advanced technology industries included in the dual-use classification must consider alternative measures to address this complex and important area of law. The United States is recognized as a leader in technological innovations,[11] yet companies operating within the U.S. are constantly restrained by Export Control requirements.[12] These requirements delay corporate transactions by requiring that companies must perform due diligence about the conduct, nationality, and items' end use internally and with their customers'. The constant broadening of Export Controls is likely to result in companies leaving the United States or prioritizing the development of technology that is not subject to heightened regulation. Additionally, this protectionist policy serves as a further incentive for regulated countries, such as China, to strive for technological self-sufficiency.[13] Both results are contrary to the federal government's initiative that U.S. companies retain a dominant global position in SME and other emerging industries.

One possible solution is blockchain technology. The research and funding of blockchain technology have exponentially increased since Bitcoin first brought the technology to the international stage.[14] Potential applications of blockchain have emerged in various sectors from finance, energy, government, real estate, health care, and even international trade.[15] The application of blockchain and distributed ledger technology has the capability to revolutionize industries by providing more efficient methods and rapid transactions and record keeping.[16]

This Note analyzes the constitutionality of the deemed export requirement and proposes blockchain technology as a solution for businesses to comply with Export

---

status is determined by the Attorney General as essential for an employer to do business with any U.S. government).

[11] Walter Isaccson, *How America Risks Losing Its Innovation Edge*, TIME (Jan. 3, 2019), https://time.com/longform/america-innovation/; *America Will Dominate the Industries of the Future*, THE WHITE HOUSE: INFRASTRUCTURE AND TECH. (Feb. 7, 2019), https://www.whitehouse.gov/briefings-statements/america-will-dominate-industries-future/.

[12] LaRocca & Bass, *supra* note 4; Jenny Leonard & David McLaughlin, *U.S. Presses Ahead on Plan to Limit High-Tech Exports*, BLOOMBERG (Dec. 11, 2018), https://www.bloomberg.com/news/articles/2018-12-11/u-s-plan-to-limit-high-tech-exports-forges-on-amid-trade-truce.

[13] *Open standards, not sanctions, are America's best weapon against Huawei*, THE ECONOMIST, Apr. 11, 2020 at 10, https://www.economist.com/leaders/2020/04/08/open-standards-not-sanctions-are-americas-best-weapon-against-huawei.

[14] Jesse Yli-Huumo et al., *Where Is Current Research on Blockchain Technology?—A Systematic Review*, PLOS ONE, Oct. 3, 2016, at 9–10; Dave Berson & Susan Berson, *Blockchain Law 101: Understanding Blockchain Technology and the Applicable Laws*, 88 J. KAN. B. ASSN. 40, 40 (2019).

[15] *Distributed Ledger Technology: Beyond Block Chain*, U.K. GOV'T OFFICE FOR SCI., 64–71 (2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf; Katharine Gammon, *Experimenting with Blockchain: Can One Technology Boost Both Data Integrity and Patients' Pocketbooks?*, 24 NATURE MED. 378, 381 (2018); Mike Orcutt, *How Blockchain Could Give Us a Smarter Energy Grid*, MIT TECH. REV. (Oct. 16, 2017), https://www.technologyreview.com/s/609077/how-blockchain-could-give-us-a-smarter-energy-grid/.

[16] Marco Iansiti & Karim R. Lakhani, *The Truth About Blockchain*, HARV. BUS. REV. 118 (Jan.–Feb. 2017).

Controls. Part II explains the licensing requirements of Export Controls and the impacts the current policy has on business and employees. Part III considers the constitutionality of Export Controls under an Equal Protection Analysis in light of the national security and foreign policy considerations. This Note takes the position that export control regulations are constitutional when tailored around the protection of information related to national security—rather than economic policy based on the national origin of the employee. Part IV, irrespective of the constitutional analysis, proposes that the application of blockchain technology has a potential solution for businesses to comply with export laws. This section begins with an overview of blockchain and how this technology applies to Export Controls. It then evaluates the benefits and challenges associated with integrating blockchain technology to data security systems. Lastly, Part IV explains how the blockchain addresses national security concerns and why companies using this technology will obtain more deemed export licenses.

II. BACKGROUND: U.S. EXPORT CONTROLS

The two relevant regulations are the International Traffic in Arms Regulations (the "ITAR") and the Export Administration Regulations (the "EAR"). The ITAR and EAR are created by different congressional acts, enforced by different government agencies, and tasked with regulating different exports. Both laws seek to promote the general policy of protecting United States defense technology from going to foreign adversaries.[17] However, these regulations are also based on economic considerations.[18] Export Regulations are mainly executed through licensing requirements.[19] One way to trigger the license requirement is by exporting regulated technology, software, and equipment to a foreign person.[20] This transfer requires a license because Export Controls deem this a transfer to the foreign person's country of citizenship.[21] A license is also required when technology is reexported or transferred outside of the United States and then is released to a foreign person. While these definitions appear simple enough, compliance with Export Controls is notoriously complex.

Export Controls substantially burden corporate supply chains. For example, if Pied Piper released their regulated source code to the Chinese National engineer, this transfer is considered an export and a license would be required to make the release. If Pied Piper were to transfer their source code to a supplier in Europe and the supplier had Chinese Nationals working on the project, this is considered a reexport and a license is required to make this release. In other words, companies subject to Export Controls must obtain the required authorizations internally, with customers, with vendors, and even to visitors or affiliates of employees. As a result, companies have expanded their workforce and operations dedicated to ensure that the business remains compliant with Export Controls.[22]

---

[17] *See* 22 C.F.R. § 120.3; 15 C.F.R. § 730.6.
[18] *See* NAT'L SEC. COMM'N ON ARTIFICIAL INTELLIGENCE, *supra* note 3, at 4–6.
[19] *See* 22 C.F.R. § 120.20; 15 C.F.R. § 730.7
[20] 22 C.F.R. § 120.17; 15 C.F.R. § 734.13.
[21] 22 C.F.R. § 120.17; 15 C.F.R. § 734.13.
[22] Andrea Stricker & David Albright, *U.S. Export Control Reform: Impacts and Implications for Controlling the Export of Proliferation-Sensitive Goods and* Technologies, INST. FOR SCI. AND INT'L. SEC. (May 17, 2017), https://isis-online.org/uploads/isis-

Failure to comply with any license requirement can result in significant civil and criminal penalties—including imprisonment—to all individuals involved in the export.[23] Depending on the severity of the violations, companies that violate Export Controls may also lose exporting privileges, effectively ending business operations.[24]

A. International Traffic in Arms Regulations

The ITAR regulates the export of a broad range of technology that is deemed a defense article or service. Pursuant to the Arms Export Control Act (the "AECA"), the President has authority to "control the export and import of defense articles and defense services."[25] The ITAR is primarily administered through the Directorate of Defense Trade Controls (the "DDTC"), because the AECA delegates this authority to the Secretary of State.[26] The Department of State, in concurrence with the Department of Defense, determines what items are designated as defense articles or services.[27] Defense articles and services include technology defined under the U.S. Munitions List ("USML")[28] and technology deemed to provide "a critical military or intelligence advantage" to warrant regulation.[29] ITAR does not consider the intended use of the export—such as military or civilian purposes—in determining whether the item is subject to regulations.[30]

Corporate supply chains can trigger the license requirement under the ITAR when exporting to citizens of foreign nations, based on the citizenship of the person receiving the exports. Under the ITAR, a license from DDTC is required to export[31] or reexport[32] any technical data or defense article to a foreign person or foreign end-use.[33] "Technical data" includes information required for the "design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification" of a defense item or software directly associated with defense articles.[34] The ITAR defines a "foreign person" as any natural person that is not a citizen or lawful permanent resident of the United States.[35]

---

reports/documents/Export_Control_Reform_Initiative_Review_and_Recommendations_May_2017_Final.pdf.

[23] 22 C.F.R. § 120.27; 15 C.F.R. § 764.3.

[24] 22 C.F.R. § 120.27; 15 C.F.R. § 764.3.

[25] 22 C.F.R. § 120.1(a).

[26] *Id.* at (b)(2).

[27] 22 C.F.R. § 120.2.

[28] Cecil Hunt, *Understanding the Rules of Trade*, TRADEPORT, (Dec. 2006), https://tradeport.org/index.php/trade-toutorials-130?id=67. *See also* 22 C.F.R. § 120.3(a) (describing "items specifically designed or modified for military use, but designations and determinations have extended ITAR jurisdiction to some items with non-military use as well" such as semiconductor memory and logic chips.).

[29] 22 C.F.R. § 120.3(b).

[30] 22 C.F.R. § 120.3.

[31] 22 C.F.R. § 120.17(a)(2). Export, among other things, includes "releasing or otherwise transferring technical data to a foreign person" in the U.S. (a "deemed export").

[32] 22 C.F.R. § 120.19(a)(2). Reexport includes the "release of technical data to a foreign person" that is a citizen of a country different from the foreign country that the release takes place (a "deemed reexport"). *Id.*

[33] 22 C.F.R. § 127.1(a).

[34] 22 C.F.R. § 120.10(a).

[35] 22 C.F.R. § 120.16. This definition includes "any foreign corporation, business association, partnership, any other entity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments." *Id.*

To address the strict ITAR regulations, companies like Boeing implement rigorous security measures. Companies hire armed guards to monitor the perimeter of research and manufacturing facilities.[36] The employees work on limited scope projects rather than building the entire product.[37] At Boeing, for example, employees are hired to work on a particular wing for a plane. Additionally, the company's information only allows for single person computer access. The heightened regulation hinders foreign nationals' employment opportunities, and the pool of qualified candidates and companies would prefer to simply hire U.S. persons to avoid all the extra security measures. The employment issue expands beyond commercial operations as academic institutions working on regulated technology are also subject to these regulations.[38]

B. Export Administration Regulations

The EAR regulates a broad spectrum of items including commercial, "dual use" and certain military goods, equipment, materials software and technology.[39] The EAR is promulgated pursuant to the Export Control Reform Act (the "ECRA") as of August 2018, formerly the Export Administration Act ("EAA") and International Emergency Economic Powers Act ("IEEPA") during the EAA lapse.[40] The Department of Commerce administers the EAR through the Bureau of Industry and Security ("BIS").[41] Items subject to the EAR include all U.S. origin items regardless of location, including foreign-made products that incorporate U.S. origin commodities and foreign-made products directly based on U.S. origin technology or software.[42] The EAR also applies to items produced outside of the U.S. that incorporate more than *de minimis* controlled U.S. content.[43]

There are four primary factors that determine whether a license is required: (1) the item exported; (2) where the export is going; (3) who is involved in the transaction; and (4) the item's use. The first step in the license determination process is to determine the Export Control Classification Number ("ECCN") of the item. ECCNs are categorized on the Commerce Control List ("CCL"). If the item does not fall into any of the categories, then the item is labeled as EAR99. The second step is to consider the country of destination by referencing the CLL Country Chart.[44] Under the current regulations a license is unlikely to be granted for embargoed countries. Third, businesses must consider who is the intended end-user and which individuals are involved in the transactions. The last step in the license determination process is to review the end use of the item. If a license requirement exists,

---

[36] *See What is an ITAR Controlled Facility*, NEWSTREAM ENTERS.: NEWSTREAM BLOG (Oct. 31, 2019, 12:50 PM), https://www.newstreaming.com/blog-hub/what-is-an-itar-controlled-facility.

[37] *See* Martin Horan, *Data Security Best Practices for ITAR Compliance*, FTP TODAY (Oct. 9, 2019), https://www.ftptoday.com/blog/data-security-best-practices-for-itar-compliance.

[38] Julie T. Norris, *Export Controls: The Challenge for U.S. Universities*, https://www.uh.edu/research/compliance/export-controls/Export_Controls_PPT.pdf.

[39] *See* 15 C.F.R. § 730.3.

[40] 15 C.F.R. § 730.2.

[41] 15 C.F.R. § 730.1.

[42] Geroge R. Tuttle, *U.S. Controls on the Texport and Re-export of U.S. Origin Goods & Technology - EAR*, https://www.tuttlelaw.com/subjects/us_control_exp_re-exp_orig_of_tech/us_control_exp_re-exp_orig_of_tech_ear.html (last visited Sep. 28, 2020); *see also* 15 C.F.R. § 734.3.

[43] 15 C.F.R. § 734.3(a); 15 C.F.R. § 734.4 (providing a ten percent threshold for exports to Cuba, Iran, North Korea, Sudan, and Syria and a twenty-five percent threshold for all other destinations).

[44] 15 C.F.R. § 738.4(a).

then companies should review the license exceptions to see if they may proceed without a license under a particular license exception. Absent any license exception, a license must be obtained before any export occurs by filing a BIS-748P form.

Corporate supply chains can trigger the license requirement under the EAR when exporting to citizens of foreign nations. An export and reexport is defined as any release of regulated technology or source code to a foreign person (a "deemed export").[45] However, one distinction from the ITAR, is that the release of U.S. technology is considered an export to only the foreign person's current country of citizenship and residency.[46] A foreign person under EAR is synonymous with a foreign person defined in the ITAR—any natural person, company, or government that is not a citizen or lawful permanent resident of the United States—and with the phrase foreign national used in EAR.[47]

The EAR impacts more companies than the ITAR because of the "dual-use" catchall. The companies vary from cutting-edge startups to large companies like Intel. Due to the broad inclusion of the regulations, companies do not implement solidified security measures like those subject to the ITAR. Additionally, the unpredictability of the EAR makes it difficult for companies to develop any plans. The EAR includes emerging technologies or new technologies that could be used in a military capacity but are not currently associated with weapons. An example of this would be drones. Drones are a new technology that is not associated with defense or weapons, but the technology has clear military applications—a bomb could be added and dropped from a drone.

Alternatively, the EAR does not include foundational technology or older technology commonly found in the marketplace. This is largely because such technology is widely available to foreign adversaries. The fluctuation and depreciation of technology makes it difficult to quickly establish adequate regulations that address national security concerns. The federal government must remain knowledgeable of all cutting-edge U.S. technology to address potential national security concerns before foreign adversaries receive the technology. For example, how could a government regulate AI and super computers? The government's analysis usually focuses on the key components required to create the final product. However, under a protectionist policy and especially for emerging technology, the regulations favor overinclusion. These broad Export Controls allow the federal government to regulate technology before understanding its capabilities. However, even if the emerging technologies capability is ultimately limited to commercial use, there is little incentive to withdraw such regulations.

C. Impacts on Businesses and Employees

The rigorous application of deemed export requirements under the Trump Administration have hindered employers from seeking licenses for employees characterized as "foreign persons." According to the data released by BIS, over eighty-four percent of the deemed export applications were approved in 2018.[48] However, this number

[45] 15 C.F.R. § 734.13(a)(2); 15 C.F.R. § 734.14(a)(2).
[46] 15 C.F.R. § 734.13(b); 15 C.F.R. § 734.14(b).
[47] 15 C.F.R. § 772.1.
[48] *2018 Statistical Analysis of BIS Licensing – Deemed Export 2013-2018*, U.S. DEPT. OF COMMERCE, BUREAU OF INDUS. AND SEC. (Mar. 5, 2019), https://www.bis.doc.gov/index.php/documents/technology-evaluation/ote-data-portal/licensing-analysis/2410-2018-statistical-analysis-of-bis-licensing-pdf/file.

is deceiving. In 2017, BIS approved a record 1,394 deemed export licenses.[49] This record year was followed by an approval of less than 850 licenses in 2018.[50] The changes in the geopolitical climate have noticeably impacted the administration of Export Controls.

The disparity for Chinese Nationals attempting to obtain licenses is even more skewed. Chinese Nationals are far and away the most common example of licenses approved by BIS, accounting for more than over one-third of all deemed export licenses.[51] In 2018, Chinese Nationals accounted for the most commonly deemed export license approved by BIS, totaling 350. The Top ECCN for 2018 is the 3E001 license for products in the SME industry.[52] This number is less than half of the 771 licenses granted to Chinese Nationals in 2017.[53] For reference, the countries with the next highest deemed export license approval are Iran and India, countries that account for a combined 25 percent of licenses. Though Iran obtained less than 200, the deemed export numbers for Iran have largely remained consistent since 2013.[54] The decline in approved deemed export licenses is a direct representation of both the federal government's protectionist policy and the challenges U.S. businesses must undergo to hire qualified foreign nationals. Why would a company hire a foreign national that requires a deemed export license when a U.S. citizen could perform the exact same job without any Export Controls requirements?

To avoid the licensing requirement, U.S. companies began limiting employment opportunities to only U.S. citizens. The Department of Justice recently found that three different companies—a manufacturer, law firm, and engineering firm—unlawfully required job candidates to be U.S. citizens or permanent residents.[55] The law firm, Clifford Chance US LLP, argued that these hiring decisions were made in "good faith."[56] The DOJ rejected this argument, stating that no such exception exists in the federal anti-discrimination law.[57] This prohibits companies from requiring U.S. citizenship to proceed in the employment process—regardless of whether the employer intends to hire someone not subject to Export Controls. This makes it difficult for companies to hire the best and brightest candidates while also complying with Export Controls and anti-discrimination laws.[58]

Export Controls are implemented to prevent foreign adversaries from obtaining U.S. weapons and technology, thus promoting cooperation with American allies and U.S. foreign policy.[59] As noted in the National Security Commission on Artificial Intelligence, SME requires extensive expertise and financial support to develop the necessary

---

[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] U.S. DEPT. OF COMMERCE, BUREAU OF INDUS. AND SEC., *supra* note 48.
[55] Clifford Chance US LLP, DJ# 197-16-492 (U.S. Dep't of Just. Aug. 29, 2018), https://www.justice.gov/opa/press-release/file/1090596/download [hereinafter *Clifford Chance Settlement Agreement*]; Honda Aircraft Co., DJ# 197-54M-69 (U.S. Dep't of Just. Feb. 1, 2019), https://www.justice.gov/opa/press-release/file/1126521/download; Setpoint Sys., Inc., DJ # 197-77-123 (U.S. Dep't of Just. Jun. 19, 2018), https://www.justice.gov/opa/press-release/file/1072981/download.
[56] *Clifford Chance Settlement Agreement*, *supra* note 55, at 1.
[57] *Id.*
[58] *See* Chris Richard et al., *Looming Talent Gap Challenges Semiconductor Industry*, SEMI, https://www.semi.org/en/connect/workforce-development/SEMI_Deloitte_WF_Study_2017.
[59] *See* NAT'L SEC. COMM'N ON ARTIFICIAL INTELLIGENCE, *supra* note 3, at 41.

infrastructure. Currently, "[a]bout 90 percent of the SME industry is located in the United States, Japan, and the Netherlands."[60] The federal government contends that extensive regulations to the SME industry, which is dominated by the U.S. and American allies, provides "that small group of allies a major advantage."[61] While this advantage is likely true in the short-term, the long-term impact of this protectionist foreign policy may not only hinder global technology advancements but also end the United States' control over the SME industry.

Early signs indicate the beginning of the United States' decline in the SME industry. Intel recently announced concerns over the manufacturing process of 7-nanometer transistors, the most advanced chip on the market, and agreed to outsource chip manufacturing to TSMC, a Taiwanese competitor.[62] This is significant because for decades Intel led the chip industry. However in 2018, Intel's decline in the SME industry first became apparent when TSMC began manufacturing the 7-nanometer chip while Intel was struggling to bring the previous generation 10-nanometer chip to market.[63] If protectionist foreign policy is to succeed, then U.S. companies must retain the dominance in cutting-edge technology and not rely on outsourcing manufacturing to foreign competitors.

III. EQUAL PROTECTION ANALYSIS

The constitutionality of the Export Controls depends on three pivotal questions. First, what type of classification is created by Export Controls? Second, what level of scrutiny should courts apply to Export Controls? Lastly, what is the federal government's interest: national security or economic policy? Before a court, or this Note, can address these questions, there are preliminary considerations and background required to determine whether an Equal Protection analysis is applicable to export controls. Additionally, it is important to note that if a court was to consider the constitutionality of a specific deemed export license, the holding would likely be limited to the facts of the case and regulation in question. Precedent from such cases is likely because Export Controls create distinct classifications, and the regulations are based on various government interests.

As set forth more fully below, this section will analyze whether the Equal Protection Clause applies to export controls, the appropriate standard of review, the merit of the government's interest, and whether the Export Controls are properly tailored to this government purpose.

A. The Equal Protection Clause Applies to Export Controls and Regulations

The Equal Protection Clause applies to the federal laws and regulations responsible for the deemed export license requirements. Under the Fourteenth Amendment of the United States Constitution, "[n]o State shall . . . deny to any person within its

---

[60] *Id.*
[61] *Id.*
[62] Arjun Kharpal, *TSMC Jumps Nearly 10% Adding $34 billion in Value as Intel Faces Next-Generation Chip Delays*, CNBC (July 27, 2020), https://www.cnbc.com/2020/07/27/tsmc-shares-jump-as-intel-faces-next-generation-chip-delays.html.
[63] Eamon Barrett, *Intel's Decline Makes Rival Chipmaker TSMC the World's 10th Most Valuable Company*, FORTUNE (July 28, 2020), https://fortune.com/2020/07/28/intel-7nm-delay-tsmc-stock-shares-worlds-tenth-most-valuable-company/.

jurisdiction the equal protection of the laws." [64] The language of the Fourteenth Amendment suggests that the Equal Protection Clause only applies to the States and requires state action.[65] However, the United States Supreme Court has applied the Equal Protection Clause of the Fourteenth Amendment against the federal government through the Due Process Clause of the Fifth Amendment.[66] Pursuant to the Fifth Amendment, "[n]o person shall be . . . deprived of life, liberty, or property, without due process of law."[67] This is not to suggest that due process and equal protection rights are interchangeable, rather that "[t]he 'equal protection of the laws' is a more explicit safeguard of prohibited unfairness than 'due process of law.'"[68] The logic behind this application of constitutional protections is that if a law violates equal protection then it also violates due process.

The constitutional right of equal protection applied to all people living in the United States, however, is unlikely to include foreign employees working outside the United States. All U.S. residents—whether a citizen or non-citizen—are considered a "person" under the Fourteenth and Fifth Amendment. Under the Fourteenth Amendment, "[a]ll persons born or naturalized in the United States and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall . . . deny *to any person within its jurisdiction* equal protection of the laws." [69] Although constitutional protections expand beyond citizenship, equal protection rights are not afforded the same force and effect outside of United States territory.[70] For example, after World War II, the Supreme Court in *Johnson v. Eisentrager* held that German nationals had no right to a writ of habeas corpus.[71] Furthermore, the Court rejected the interpretation that the term "any person" used in the Fifth Amendment spread to all alien enemies.[72] Here, Export Controls are based around protecting U.S. weapons and advanced technology. Accordingly, a court would likely follow similar reasoning in rejecting an equal protection claim from a nonresident alien that worked for a U.S.-based company or with U.S. technology. Since aliens do not enjoy the same advantage as residents,[73] a nonresident alien is unlikely to succeed on equal protection grounds—even if the challenger has substantial connections to the United States.[74]

---

[64] U.S. CONST. amend. XIV, § 1 (emphasis added).
[65] *See id.*
[66] *See* Bolling v. Sharpe, 347 U.S. 497, 499–500 (1954) (holding that although the Fifth Amendment does not contain an equal protection clause, "it would be unthinkable that the same Constitution would impose a lesser duty on the Federal Government."); Weinberger v. Wiesenfeld, 420 U.S. 636, 638 n.2 (1975) ("This Court's approach to Fifth Amendment equal protection claims has always been precisely the same as to equal protection claims under the Fourteenth Amendment.").
[67] U.S. CONST. amend. V.
[68] Adarand Constructors, Inc. v. Pena, 515 U.S. 200, 215 (1995) (quoting *Bolling*, 347 U.S. at 499).
[69] U.S. CONST. amend. XIV, § 1 (emphasis added).
[70] *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 269 (1990); Johnson v. Eisentrager, 339 U.S. 763, 770-71 (1950).
[71] *Johnson*, 339 U.S. at 790.
[72] *Id*. at 782-83.
[73] Mathews v. Diaz, 426 U.S. 67, 78 (1976).
[74] *Verdugo-Urquidez*, 494 U.S. at 271.

B. Export Controls Impose a Suspect Classification and is Subject to Heightened Scrutiny

The Equal Protection Clause arises when government classifications impose an exclusive burden or benefit to one group of persons.[75] Legislation can create classifications either facially or in effect. Facial classifications occur when the face of the statute creates the classification.[76] Alternatively, the Equal Protection Clause is also applicable to laws that are facially neutral but create burdensome classifications in effect.[77] The Supreme Court has repeatedly held that racial classifications are reviewed under strict scrutiny.[78] For legislation to be constitutional under a strict scrutiny the laws must be narrowly tailored to further a compelling government interest.[79]

Deemed export requirements facially categorize people based on alienage; however, the application of Export Controls' in effect creates classifications based on national origin.[80] Citizenship and national origin are distinct legal classifications; however, this distinction creates inconsistency that ultimately result racial and national origin classifications. For this reason, the Supreme Court extended strict scrutiny to national origin classifications.[81] Beyond simple inconsistencies in how other countries determine citizenship, a rational basis test is inappropriate because the role of the judiciary is to protect "discrete and insular minorities."[82] For example, under the Nationality Law of the People's Republic of China, a "Chinese citizen" is defined as a person of Chinese nationality.[83] Additionally, China does not recognize dual citizenship.[84] In other words, a person of Chinese descent is considered a Chinese citizen, so long as they have not formally changed nationalities. Such fluidity between citizenship and national origin throughout the world supports the applicable of strict scrutiny because the deemed export requirement expressly—or at the very least in effect—classifies people based on race and national origin.

The determination of classification imposed by Export Controls and in turn, the appropriate standard of review, is further complicated by Executive and Legislative powers to regulate foreign affairs. Congress has plenary power over the immigration and

---

[75] *E.g.*, San Antonio Indep. Sch. Dist. v. Rodriguez, 411 U.S. 1, 59–60 (1973) (Stewart, J., concurring) ("The function of the Equal Protection Clause, rather, is simply to measure the validity of classifications created . . . .").

[76] *See, e.g.*, Brown v. Bd. of Educ., 347 U.S. 483 (1954) (rejecting racial segregation in public schools); Strauder v. West Virginia, 100 U.S. 303 (1879) (eliminating limitation of "only white male persons" for jury service).

[77] *See, e.g.*, Shapiro v. Thompson, 394 U.S. 618 (1969) (holding that durational residency requirement in effect divided applications into two groups); Harper v. Va. Bd. of Elections, 383 U.S. 663 (1966) (holding that poll taxes in effect divided voters into two groups).

[78] Adarand Constructors, Inc. v. Pena, 515 U.S. 200, 227 (1995); Gratz v. Bollinger, 539 U.S. 244, 270 (2003).

[79] *Pena*, 515 U.S. at 227.

[80] *See supra* Part II A, B.

[81] City of Cleburne, Tex. v. Cleburne Living Ctr., 473 U.S. 432, 440 (1985).

[82] U.S. v. Carolene Prod. Co., 304 U.S. 144, 152 n.4 (1938) (stating that strict scrutiny is required for laws implicating a fundamental right or suspect class).

[83] *General Information on Chinese Nationality*, HONG KONG IMMIGRATION DEP'T. (last updated Jan. 20, 2017), https://www.immd.gov.hk/eng/services/chinese_nationality/general_info.html.

[84] *Nationality Law of the People's Republic of China*, EMBASSY OF THE PEOPLE'S REPUBLIC OF CHINA IN THE U.S., http://www.china-embassy.org/eng/ywzn/lsyw/vpna/faq/t710012.htm (last visited Sep. 19, 2020).

naturalization process,[85] and the power to regulate commerce among foreign nations.[86] Generally, these legislative powers are "immune from judicial control."[87] However, the Supreme Court has interpreted the phrase "within its jurisdiction" broadly, and have repeatedly found that resident aliens also enjoy constitutional protections.[88] Additionally, the Executive has broad authority when regulating foreign nationals because the President has constitutional obligations to regulate foreign affairs. In *Trump v. Hawaii*, the Supreme Court recognized that there is minimal judicial review of Executive actions concerning foreign nationals because courts generally lack the competency to determine national security questions.[89] Any judicial action regarding foreign nationals entering the country and national security must be highly constrained because any action that would "inhibit the flexibility of the President to respond to changing world conditions should be adopted only with the greatest caution."[90] Export controls, however, are not related to whether foreign nationals are allowed to enter into the country; rather, the deemed export-licensing requirement affects individuals who are already in the United States legally and seeking employment in regulated industries.

Since Export Controls arise from congressional acts delegating to executive agencies the authority to regulate various exports, a court may not apply strict scrutiny but rather some form of heightened scrutiny in these cases. Accordingly, Export Controls must, at the very least, be necessary to achieve an important government interest.[91]

C. Export Controls are Broadly Tailored around a Compelling Government Interest

The government must satisfy two prongs under a heightened scrutiny analysis. First, the government has the burden of showing that the classification is based on a compelling interest.[92] Second, the laws must be narrowly tailored to achieve the compelling interest.[93] Both prongs empower courts to ensure lawmakers are "pursuing a goal important enough to warrant [the] use of a highly suspect tool."[94] Courts should not blindly defer "to legislative or executive pronouncements of necessity" in an equal protection analysis."[95] This section first considers the government's interest in protecting advanced U.S. technology from China through deemed export license, then considers whether the licensing requirements are narrowly tailored to address their concerns.

---

[85] U.S. CONST. art. I, § 8, cl. 4.
[86] *Id.* at art. I, § 8, cl. 3.
[87] Fiallo v. Bell, 430 U.S. 787, 792 (1977) (quoting Shaughnessy v. Mezei, 345 U.S. 206, 210 (1953)).
[88] *See* Yick Wo v. Hopkins, 118 U.S. 356, 369 (1886) (holding that the Fourteenth Amendment protects resident aliens); Mathews v. Diaz, 426 U.S. 67, 77 (1976) (holding that the Fifth and Fourteenth Amendments protect illegal or involuntary aliens within the jurisdiction of the United States); Plyler v. Doe, 457 U.S. 202, 211–12 (1982) (holding that the Fourteenth Amendment's Equal Protection Clause protects illegal aliens).
[89] Trump v. Hawaii, 138 S. Ct. 2392, 2419 (2018).
[90] *Id.* (quoting *Mathews*, 426 U.S. at 81–82).
[91] Graham v. Richarson, 403 U.S. 365, 376 (1971); Bernal v. Fainter, 467 U.S. 216, 219 (1984); In re Griffiths, 413 U.S. 717 (1973).
[92] Johnson v. California, 543 U.S. 499, 505 (2005) (classifications are inherently suspect because they "raise special fears that they are motivated by an invidious purpose.").
[93] *Id.*
[94] Adarand Constructors, Inc. v. Pena, 515 U.S. 200, 226 (quoting City of Richmond v. J.A. Croson Co., 488 U.S. 469, 493 (1989)).
[95] *J.A. Croson Co.*, 488 U.S. 469, at 501.

i. Compelling-Interest Prong

The federal government contends that preventing Chinese espionage and intellectual property theft, particularly in the semiconductor industry, is vital to national security. Since 2011, more than 90 percent of Americans prosecuted for economic espionage had ties to China.[96] At the end of 2019, a cancer researcher at a Harvard research center was arrested for allegedly smuggling information to China.[97] On May 3rd, 2019, in the biggest trade secret infringement case in history, the Superior Court of the State of California ordered an $845 million judgment against XTAL Inc., a semiconductor manufacture.[98] The jury found XTAL guilty of stealing trade secrets from ASML US Inc., the United States branch of the largest supplier of photolithography systems in the semiconductor industry.[99] XTAL was founded by two long time employees of Brion Technologies, a light source company that was later acquired by ASML.[100] The court found that prior to leaving Brion, these engineers copied company information onto an external storage device.[101] This case exemplifies the importance of company security measures that limit an employee's access to and transferability of regulated information. Additionally, this example supports the federal government's concern regarding foreign adversaries obtaining U.S. technology. Semiconductor companies such as ASML, Intel, and TSMC are the driving forces behind Moore's law, or the exponential increase in transistors on computer chips every 18 months.[102]

The United States is not alone in its distrust of China's business and politics; this is a feeling shared by most Western countries.[103] In an effort to block ASML from selling a machine to China, President Trump sent Secretary of State Mike Pompeo to pressure the Dutch Prime Minster into granting an export control license.[104] Secretary Pompeo even provided the Dutch leader with a classified intelligence report.[105] This defensive maneuver by the White House indicates that the protection of semiconductor technology from China is not only a compelling interest for the United States, but also internationally. Ironically,

---

[96] *The new red scare on American campuses*, THE ECONOMIST, Jan. 2, 2020, https://www.economist.com/briefing/2020/01/02/the-new-red-scare-on-american-campuses [hereinafter *Red Scare*].
[97] *Id.*
[98] Mike LaSusa, *ASML Scores $845M IP Judgment Against Bankrupt XTAL*, LAW360 (May 6, 2019), https://www.law360.com/articles/1156580/asml-scores-845m-ip-judgment-against-bankrupt-xtal.
[99] *Id.*
[100] Kieren McCarthy, *Crystal Balls Up: Chip Design Shop XTAL Must cough up $223m for Pinching Trade Secrets*, THE REGISTER (Dec. 3, 2018), https://www.theregister.co.uk/2018/12/03/xtal_asml_judgment/.
[101] *Id.*
[102] Rachel Courtland, *Leading Chipmakers Eye EUV Lithography to Save Moore's Law*, IEEE SPECTRUM (Oct. 31, 2016), https://spectrum.ieee.org/semiconductors/devices/leading-chipmakers-eye-euv-lithography-to-save-moores-law.
[103] *Why Chinese officials like useless meetings in Over-stuffed chairs*, THE ECONOMIST, Aug. 3, 2019, https://www.economist.com/china/2019/08/01/why-chinese-officials-like-useless-meetings-in-over-stuffed-chairs [hereinafter *Armchair Warriors*].
[104] Alexandra Alper, Toby Sterling, & Stephen Nellis, *Trump administration pressed Dutch hard to cancel China chip-equipment sale: sources*, REUTERS (Jan. 5, 2020), https://www.reuters.com/article/us-asml-holding-usa-china-insight/trump-administration-pressed-dutch-hard-to-cancel-china-chip-equipment-sale-sources-idUSKBN1Z50HN.
[105] *Id.*

most American electronic devices are assembled in China.[106] Often however, these Chinese firms are utilizing foreign suppliers to provide advanced technology such as robotics, cloud computing, and semiconductors. This disparity is most notable in semiconductors, as China imports nearly all of its semiconductor equipment from foreign companies. Currently, China lacks the infrastructure and technical know-how to compete in this market. Experts have estimated that China would need at least ten years, but likely more, to develop competitive computer chip facilities.[107]

The modern-day arms race is not fought on the battlefield but rather through intrusion software. In November, the federal government began a national-security review of ByteDance, a Chinese company and owner of the popular video app TikTok.[108] Last year, TikTok was downloaded more than 750 million times.[109] ByteDance's connection to China brings up issues regarding data geopolitics and information transfer from the United States to China, an issue that is largely the reason for the sanctions against Huawei, a Chinese telecom manufactory. These spies are not the James Bond type—they can vary from students, to academics, to entrepreneurs, to even journalists.[110] By requiring licenses before receiving regulated U.S. technology, companies must perform due diligence to ensure their customers intend to use the export for civilian purposes. However, this is easier said than done, because in countries like China, the funding and research of commercial sectors are often intertwined with military efforts.[111]

ii. Narrowly Tailored Means Prong

Under a heightened scrutiny analysis, it is likely unconstitutional for the federal government to create nationality classifications when the government's interests are tailored around economic policy. When it comes to military authority the Supreme Court has applied an "exceedingly deferential" approach. After World War II in *Korematsu v. United States*, the internment camps from Japanese Americans was upheld under the Equal Protection Clause.[112] Although this case was widely criticized, the context of a world war is distinguishable from the current situation [113] The United States should not succumb to

---

[106] Anna-Katrina Shedletsky, *Made In China? Three Trends Driving Electronics Manufacturing In 2019*, FORBES (Jan. 24, 2019), https://www.forbes.com/sites/annashedletsky/2019/01/24/made-in-china-three-trends-driving-electronics-manufacturing-in-2019/#493002272903.

[107] Danny Vincent, *How China plans to lead the computer chip industry*, BBC NEWS (Nov. 19, 2019), https://www.bbc.com/news/business-50287485.

[108] *TikTok's silly clips raise some serious questions*, THE ECONOMIST, Nov. 7, 2019, https://www.economist.com/business/2019/11/07/tiktoks-silly-clips-raise-some-serious-questions.

[109] *Id.*

[110] *The shape-shifting threat of Chinese espionage*, THE ECONOMIST, Nov. 21, 2019, https://www.economist.com/books-and-arts/2019/11/21/the-shape-shifting-threat-of-chinese-espionage [hereinafter *Chinese Espionage*].

[111] *See* OFFICE OF THE SECRETARY OF DEFENSE, *Military and Security Developments Involving the People's Republic of China 2019*, Annual Report (May 2019), https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf ("China has mobilized vast resources to fund research and subsidize companies involved in strategic science and technology fields while pressing private firms, universities, and provincial governments to cooperate with the military in developing advanced technologies.") [hereinafter *Military and Security*].

[112] Korematsu v. United States, 323 U.S. 214, 216-19 (1944).

[113] *Armchair Warriors*, *supra* note 103.

Chinese espionage, but, at the same time, should not stray from the values of liberty and equal protection.

With broadening export control regulations, companies must perform due diligence about the conduct, nationality, and items' end use internally and with their customers. However, this is easier said than done, because in countries like China, the funding and research of commercial sectors are often intertwined with military efforts.[114] In a response to the new export rules, the Semiconductor Industry Association President, John Neuffer, recognized that "while we understand military-civil fusion trends demand smart and targeted national security responses, we are concerned these broad rules will unnecessarily expand export controls for semiconductors and create further uncertainty for our industry during this time of unprecedented global economic turmoil."[115] The global semiconductor industry accounted for over $400 billion in revenue in 2019, a decrease of twelve percent from the previous year.[116] As American companies are losing customers, suppliers, and profits, Chinese companies such as Huawei are finding alternative sources for U.S. import components.[117]

National security and foreign policy efforts by the White House to address the threat from China avoid judicial interpretation. In the modern digital world, there is no doubting that the semiconductor industry will largely impact future economic growth. However, there is no linear connection of semiconductor technology to national security. Export Controls are clouded under an umbrella of "national security," yet the impact is directed at consumer technology. These regulations all stem from the Trump Administration, which is known for impulsive actions and the use of economic sanctions in negotiations.[118] Initially, the administration and "national-security hawks" utilized the entity list to separate commercial relations from China.[119] Now, in light of future assets, the Department of Commerce implements Export Controls as the main protection of American content from China.[120]

"Liberty finds no refuge in a jurisprudence of doubt."[121] The importance of discovering spies is undeniable. However, in this effort to limit China's bad actors the United States must be democratic and vigilant when implementing regulation to protect American technology. Broad restrictions and a presumption of denial in the export process suggests that fear drives these policies—which is particularly concerning for a country

---

[114] *Military and Security*, *supra* note 111.

[115] Adam Behsudi, *A potential game changer for China export controls*, POLITICO (Apr. 28, 2020), https://www.politico.com/newsletters/morning-trade/2020/04/28/a-potential-game-changer-for-china-export-controls-787183.

[116] Semiconductor Industry Association, *Worldwide Semiconductor Sales Decrease 12 Percent to $412 Billion in 2019*, CISION PR NEWSWIRE (Feb. 03, 2020), https://www.prnewswire.com/news-releases/worldwide-semiconductor-sales-decrease-12-percent-to-412-billion-in-2019-300997962.html.

[117] *Id.*

[118] *Donald Trump's betrayal of the Kurds is a blow to America's credibility*, THE ECONOMIST, Oct. 17, 2019, https://www-economist-com.ezproxy1.lib.asu.edu/leaders/2019/10/17/donald-trumps-betrayal-of-the-kurds-is-a-blow-to-americas-credibility.

[119] *America blacklists China's best artificial-intelligence firms*, THE ECONOMIST, Oct. 10, 2019, https://www.economist.com/business/2019/10/10/america-blacklists-chinas-best-artificial-intelligence-firms.

[120] *Old export regulations get a new use*, THE ECONOMIST, Jan. 16, 2020, https://www.economist.com/united-states/2020/01/16/old-export-regulations-get-a-new-use.

[121] Planned Parenthood v. Casey, 505 U.S. 833, 843 (1992).

rooted in capitalism. Export Controls should prevent Chinese spies from creating "shadow labs" to replace American research facilities[122]; however, they should not eliminate all qualified researchers from working in the United States. This reduction of talent in the hiring process includes American universities, as there are nearly twenty universities.[123] Moving forward, the Trump Administration must work with American companies to accelerate the research and development of mobile networks. Protectionism will not allow America to "win the tech cold war," and a new approach is imperative to ensure that China does not control the global digital infrastructure.

The economic correlation of the deemed export requirement is supporting America first in the short-term. However, the long-term impacts could be detrimental to the United States role as a leader in cutting-edge technology. The lack of American innovation from companies, like Intel, will hinder the dominance of United States and American allies from competition with lower cost options provided by Chinese firms.[124] Moreover, the complexities surrounding Export Controls could drive business away from America, thus resulting in a loss of jobs, economic power, and the ability to regulate information from China.

IV. PROPOSAL: BLOCKCHAIN TECHNOLOGY

There are two options for technology companies to address U.S. Export Controls. On one hand, companies can increase their lobbying presence in Washington, D.C. and attempt to negotiate less complex and stringent regulations for emerging technologies. On the other hand, private industries can seek to establish a precedent with the federal government of receiving deemed export licenses based on limited exposure to regulated technology. This process requires, among other things, financial and labor resources dedicated to enhancing the company's IT security. In light of the two options, companies responsible for bringing cutting edge technology to market should not shy away from the opportunity to take matters into their own hands—in a multibillion-dollar industry like SEMI,[125] this would likely be the general public and federal government's perspective as well.

Creating this precedent with the federal government requires companies to revolutionize their current security system. BIS, in regards to deemed export licenses, recommended that companies write a Letter of Explanation ("LOE") describing the organizations IT security system.[126] To improve a company's likelihood of obtaining a deemed export license, the LOE must explain the internal protection mechanisms and detail the security protocols when foreign nationals are working on regulation technology.[127] Companies must show they benefit more than the employee in this transaction.[128] At the same time, this distinction of benefits obtained ensures that the foreign person's country of

---

[122] *Chinese Espionage*, *supra* note 110.
[123] *Red Scare*, *supra* note 96.
[124] *Id.*
[125] Richard et. al, *supra* note 58.
[126] *See Guidelines for Foreign National Licensing Applications*, BUREAU OF INDUSTRY AND SECURITY, https://www.bis.doc.gov/index.php/component/content/article/14-policy-guidance/deemed-exports/109-guidelines-for-foreign-national-licenses (last visited Sept. 28, 2020).
[127] *Id.*
[128] *Id.*

citizenship does not obtain general knowledge of this regulated technology. This proposal by BIS appears promising. However, when dealing with federal laws that are based on national security the federal government wants more than merely adequate parameters.

As set forth more fully below, regulated companies can utilize the transparency, immutability, and cryptography functions inherent to blockchain technology as a means to exceed the LOE recommendation by BIS. This section begins with an overview of blockchain technology and how it applies to data security. It then proposes various approaches to how businesses can integrate blockchain and why this technology would enhance current cybersecurity systems. Additionally, this section details the merits of this technology, and how it addresses the federal government's national security concerns and current issues within the SME industry. Finally, it considers the governance and confidentiality challenges and other mediums capable of achieving comparable results. Before beginning, this note recognizes that a commercial blockchain security system is not a revolutionary implementation of distributed ledge technology's potential. However, such a system can address complex issues, like Export Controls, that demand transaction efficiency and in-time record keeping.

A. Blockchain's Applications to Data Security Systems

The concept of blockchain was first made popular through Bitcoin after the inventor(s) under the name Satoshi Nakamoto published a whitepaper. Bitcoin is a decentralized cryptocurrency that allows users to engage in transactions on a peer-to-peer network without the need for a central bank to serve as an intermediary.[129] The name cryptocurrency is associated with the application of cryptographic hash functions in cryptocurrencies.[130] Cryptography has also been applied to public and private keys allowing individuals to verify their ID and ensure privacy by protecting the transaction's information.[131] The research and funding of blockchain technology has exponentially increased in recent years.[132]

Potential applications of blockchain have emerged in various sectors from finance, government, real estate, health care, and even international trade.[133] One major benefit associated with blockchain is that data entries can be accessed in real time.[134] The modern applications of blockchain and distributed ledger technology are beginning to revolutionize industries based on transactions and record keeping.[135] Constant access to information has the potential to diminish transaction times and bureaucratic delays. Another important aspect of blockchain is the government avoidance as a means to uphold privacy in the digital age. The "cyberpunk's" movement is rooted in the libertarian principles that, as a

---

[129] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf (last visited Sep. 28 2020).
[130] Dylan Yaga et al., *Blockchain Technology Overview*, U.S. NAT'L. INST. OF STANDARDS AND TECH., (Oct. 2018), https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf.
[131] *Id.* at 11.
[132] Jesse Yli-Huumo et al., *supra* note 14, at 9–10.
[133] U.K. GOV'T OFFICE FOR SCI., *supra* note 15.
[134] Lucas Mearian, *What is blockchain? The complete guide*, COMPUTERWORLD (Jan. 29, 2019), computerworld.com/article/3191077/what-is-blockchain-the-complete-guide.html.
[135] *See* Marco Iansiti & Karim R. Lakhani, *The Truth About Blockchain*, HARV. BUS. REV., 1, 3–4 (2017).

society, privacy should not be based on the good faith efforts of governments or corporations but rather in the hands of the people.[136]

Blockchains empower people by creating a trusted distributed ledger that details transactions over public networks. Put simply, a blockchain is just a ledger, similar to an excel spreadsheet, that is maintained from a decentralized network rather than through one central server.[137] This technology can be applied to almost any transfer once the digital asset and transaction protocols have been determined. While blockchain technology may not be applicable to every industry or transaction, numerous industries are enticed by the transparency and immutability functions inherent to blockchain. The transparency element allows everyone that is a part of the network to access the information in in real time.[138] By collecting all transactions, the blockchain creates an auditable record or ledge of all data transfers.[139] Once a "block" in the blockchain is created all future blocks will be formed based on the information of the previous block. This chronological ledger creates the "chain." The chain is immutable across the entire decentralized network because everyone has access to the prior records and if any block were changed then the chain would be incorrect.[140]

There are various types of blockchain that impact the network access, system scalability, and the consensus protocols of transactions. Blockchains are classified as public or private and permissioned or permissionless. From a purist libertarian point of view, like the cyberpunk's perspective, the only type of blockchain is a public permissionless chain such a Bitcoin. In a public permissionless system anyone can participant and no specific person or entity can manage the transactions on the platform. Generally in public blockchains the participants are anonymous, the scalability is low, and the computing power necessary to operate the system is high and often results in slow transaction validation periods.[141] Alternatively, blockchains classified as consortium or private permissioned only include identified participants that obtained prior authorization and are managed by a select people or entities.[142] Since a permissioned system is inherently smaller and available to less people, companies are attracted to this form of blockchain systems because they are easy to scale and allow for quick transaction speeds.[143]

B. Corporate Implementation of Blockchain

Before revolutionizing any data system, it is important for businesses to understand the vulnerabilities of current data systems and how the implementation of blockchain technology can address any weaknesses. In the highly advanced industries, such as SME, information is valuable. In turn, the protection of all proprietary information is vital. Yet, traditional security systems often apply the "security through obscurity" approach to

---

[136] *See* Eric Hughes, *A Cypherpunk's Manifesto*, ACTIVISM: CYPHERPUNKS (Mar. 9, 1993), https://www.activism.net/cypherpunk/manifesto.html.
[137] *See* Dylan Yaga et al., *supra* note 130.
[138] *Id.* at 41.
[139] *Id.* at 46.
[140] *Id.* at 34.
[141] Emmanuelle Ganne, *Can Blockchain revolutionize international trade?*, WORLD TRADE ORGANIZATION (2018), at 10, https://www.wto.org/english/res_e/booksp_e/blockchainrev18_e.pdf.
[142] *Id.* at 10–11.
[143] *Id.*

database engineering.[144] The theory behind this approach is to keep the security mechanisms a secret. However, a major problem associated with this approach is that the entire system is vulnerable if someone were to hack the security mechanism. In other words, if a security breach were to occur then all of the data is accessible, and the system could collapse. By contrast, blockchain has no single point of vulnerability. As noted by Marhsall Gerstien & Borun LLP, an intellectual property law firm, blockchain is "a distributed ledger network using public-key cryptography to cryptographically sign transactions that are stored on a distributed ledger, with the ledger consisting of cryptographically linked blocks of transactions."[145] So instead of implementing one security mechanism for the entire database, blockchain individually encrypts each transaction stored in the chain.[146]

Blockchain eliminates the internal bad actor or spy problem. Information stored on a blockchain is accessible to authorized parties, however the information on the chain can be limited to viewing while downloading or copying functions are disabled. Genomic companies are implanting this type of blockchain for DNA data storage.[147] Nebula Genomics, for example, allows third parties to access the whole-genome sequences under certain specified conditions.[148] However, the information is limited to the blockchain platform. Third parties do not have the capability to download or transfer the information for personal use, allowing consumer to utilize their genetic information in a protected system.[149] As such, employees, customers, and vendors are put in a better position to exchange or release such information.

Consortium permissioned or private blockchain systems with business-to-government (B2G) capabilities can revolutionize Export Controls compliance by allowing companies to program the system around their specific security and industry needs. The scalability of private systems allows companies[150]to access data such as internal designs, developments, productions, manufacturing, assembly, operations, repairs, testing, maintenance or modification of regulated software. The decentralized blockchain system provided heighted security because the standard centralized cloud model is susceptible to manipulation and requires companies to share data with third parties.

The cybersecurity capabilities of blockchain address the federal government's national security concerns. In a blockchain, the system maintains an immutable real-time ledger of all data transfers while also allowing different levels of access to certain users. The "super audit trail" is one of the major factors behind other industries' building and testing blockchain applications.[151] Companies subject to Export Controls have the option

---

[144] Nir Kshetri, *Blockchain's roles in strengthening cybersecurity and protecting privacy*, 41 TELECOMM. POL'Y 1027, 1028 (2017).
[145] *Id.* at 1029.
[146] Ron Ribitzky et al., *Pragmatic, Interdisciplinary Perspectives on Blockchain and Distributed Ledger Technology: Paving the Future for Healthcare*, BLOCKCHAIN IN HEALTHCARE TODAY, https://blockchainhealthcaretoday.com/index.php/journal/article/view/24/21 (last visited Sep. 28, 2020).
[147] Helen Albert, *How Blockchain Companies Are Helping Us Protect Our Genomic Data*, LABIOTECH.EU (June 26, 2019), https://www.labiotech.eu/features/blockchain-control-genomic-data/; Megan Molteni, *These DNA Startups Want to Put All of You on the Blockchain*, WIRED (Nov. 16, 2018), https://www.wired.com/story/these-dna-startups-want-to-put-all-of-you-on-the-blockchain/.
[148] Molteni, *supra* note 147.
[149] *Id.*
[150] Ribitzky, *supra* note 146, at 4.
[151] Kshetri, *supra* note 144.

of connecting the federal government to their distributed ledgers or providing a current blockchain record upon request or audit. Since the information is not stored in a single centralized location, all servers will need a consensus protocol to protect the record changes from discrepancies. The record details every transaction including the parties involved and information exchanged in an encrypted form. The transaction of information will only occur if both parties are authorized by the system. In the Export Controls context, the system could be programmed to limit access to foreign persons while providing U.S. persons not subject to regulations access to sensitive information. Such protection procedures ensure compliance with Export Controls by allowing only authorized persons to access regulated information or technology.

Additionally, blockchain technology can assist supply chain operations in complying with Export Controls by utilizing "smart contracts," coded computer functions that self-execute based on activities in the chain,[152] in transactions subject to Export Controls. For example, whenever a transaction involves delivering a dual-use technology to an employee, customer, or vendor, a smart contract could require proof of authorization or licensing prior to enabling the transaction. This system would also limit administrative costs and the potential for fraud by implementing an automated process. The interconnection of the parties' involved, including regulators, can exponentially increase international transaction speeds.[153]

C. Corporate Challenges Associated with Blockchain Systems

Blockchain offers many of benefits; however, it does present numerous, varying challenges. Export controls are constantly changing, and regulators are constantly working to account for new emerging technology. Additionally, the constant advancements in high-tech industries can make currently regulated technology obsolete in the near future. The policy and administration regarding Export Controls will always be subject to political changes in Congress and the Executive. Under President Trump, the federal government has adopted a protectionist foreign policy against China. This policy could change very soon if someone else were elected president in 2020, though it is unlikely that the federal government's concerns of espionage and economic espionage will change—even if a commercial trade agreement was established.

Implementing blockchain technology in a company's IT system is not the only way for companies to seek compliance with Export Controls. A persuasive LOE formatted around BIS's recommendations for obtaining more deemed export licenses can be obtained through an encrypted database or managed database capable of comparable features. These systems lack documentation of who accessed data when. Rather, they can only provide similar firewall mechanisms and security measures. While any data system is susceptible to hackers, companies may prefer to implement a cybersecurity strategy that will not concern stakeholders, as the value of a company is inherently tied to the risk of potential government enforcement actions.[154] Another major fault associated with blockchain is the need for more research and development of appropriate consensus models. Bitcoin

---

[152] *A Primer on Smart Contracts*, CMTY. FUTURES TRADING COMM'N., at 4 (Nov. 27, 2018), https://www.cftc.gov/sites/default/files/2018-11/LabCFTC_PrimerSmartContracts112718.pdf.

[153] Ganne, *supra* note 141, at 17–25.

[154] Will Kenton, *Regulatory Risk Defined*, INVESTOPEDIA (Jan. 12, 2018), https://www.investopedia.com/terms/r/regulatory_risk.asp.

currently utilizes a proof-of-work consensus model. This model requires a lot of computing power to validate the transactions because it must solve a computationally intensive puzzle to verify blocks on the chain.[155] This type of consensus model is not sustainable, as Bitcoin uses as much energy as the entire country of Switzerland.

V. CONCLUSION

Blockchain represents a powerful emerging technology capable of enhancing Export Controls compliance and corporate record keeping. The technology has numerous features that can address the federal government's concerns regarding U.S. technology. By providing an immutable record to a highly secure cyber system, corporations can discover bad actors before they can use any company information to steal clients or, worse, provide their information to foreign adversaries. However, the creation and implementation of a blockchain system will require businesses to devote substantial manpower and funding to address the technical challenges.

More importantly, once a blockchain system is developed, there is still no guarantee that this type of system will result in deemed export licenses. The federal government needs to work with advanced technology companies on solutions for export licensing. Highly advanced companies should not attempt to solve such a complex problem with an elementary tactic such as lobbying. Rather, businesses in the SME and other regulated industries need to reevaluate their cybersecurity to address faults in traditional methods and work with the federal government to navigate the governance challenges associated with Export Controls. The successful development of private permissioned blockchains will contribute to a robust American economy that is equipped to protect against espionage.

[155] *Bitcoin Energy Consumption Index*, DIGICONOMIST (Sept. 20, 2020), https://digiconomist.net/bitcoin-energy-consumption. Note that this source is updated continuously.