MILLING THE F/LOSS: EXPORT CONTROLS, FREE AND OPEN SOURCE SOFTWARE, AND THE REGULATORY FUTURE OF THE INTERNET

*Stav Zeitouni**

This Note investigates U.S. export controls as they relate to free and open source software (FOSS), arguing that the U.S. government has responded to the challenges of modern software by attempting to force an ill-fitting framework to accommodate FOSS. A contemporary reexamination of the state of export controls over FOSS can help in mapping out the responses generated by national security interests to the challenges of the internet. In particular, the Note offers a detailed account of the ways in which federal export controls have excluded FOSS from their regulatory purview through a powerful public availability exemption. In doing so, regulators have essentially labeled publicly available software as unthreatening to national security, regardless of the potential uses of any particular code.

Ultimately, this piece does not argue for stronger export restrictions on FOSS. Instead, it shows that current regulation does not comprehensively control FOSS and tries to tease out the implications of this regulatory approach. In particular, the Note explores apparent regulatory inconsistencies when export controls are applied to particular areas of FOSS. It argues that these inconsistencies ultimately lead to the displacement of software regulation by data regulation. Tracing the causes of this displacement allows for a deeper examination of the nuanced ways in which FOSS has altered the form and function of export controls and the ways these have altered the development of FOSS in turn. The interaction between these two facets of the digital age offers a case study in how cyber governance and the internet interplay and construct one another.

* J.S.D. Candidate, N.Y.U. School of Law. I am grateful to Thomas Streinz and Benedict Kingsbury for helping to shape the ideas for this paper in its initial stages, and for generous and useful comments later on. I am similarly indebted to Omer Feinberg, Tal Mendelson, Robert F. Roach, Ira Rubinstein, Tatiana Shapiro, David Stein, Katherine Strandburg, and the participants of the Guarini Institute's Open Source Software Workshop for helpful conversations and comments. Finally, the editorial team of the N.Y.U. Journal of Legislation & Public Policy provided invaluable feedback during the publication process of this Note. All mistakes are my own.

INTRODUCTION

The halcyon days of the early internet prompted remarkable optimism. Many people, particularly in the United States, viewed the new networked space as a freedom-reifying technology, borderless and somewhat untouchable.[1] The U.S. government was, at least outwardly, also on board with this view; beginning in the 1990s, successive administrations pioneered and exported an American internet freedom model predicated on non-regulation.[2]

Contemporary research in the U.S. and abroad has highlighted the pitfalls of an untouchable technology and proven more ambivalent regarding non-regulation.[3] Moreover, some scholars argue that technological optimism generally oversimplifies the more equivocal role technologies play in society.[4] As a result, there has been a push in both academic and political circles for more federal regulation, aimed in particular at large internet-based platforms.[5]

---

1. Well-known utopian statements to this effect include, for example, John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (1996), https://www.eff.org/cyberspace-independence; David R. Johnson & David G. Post, *And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralized, Emergent Law, in* COORDINATING THE INTERNET 62 (Brian Kahin & James H. Keller, eds. 1997).

2. Jack Goldsmith, *The Failure of Internet Freedom*, KNIGHT FIRST AMENDMENT INST. AT COLUM. U. (Jun. 13, 2018), https://knightcolumbia.org/content/failure-internet-freedom.

3. *Id.*

4. JULIE E. COHEN, BETWEEN TRUTH AND POWER 3–5 (2019).

5. *See, e.g.*, Tom Wheeler, *Facebook Says It Supports Internet Regulation. Here's an Ambitious Proposal that Might Actually Make a Difference*, TIME (Apr. 5, 2021),

Software production and distribution have become prominent targets of this increased regulation.[6] Scholars have generally focused their attention on the ways this kind of regulation affects the marketplace or interacts with what are traditionally considered paradigms of private law (property, copyright, contracts, etc.). By contrast, software regulation originating from the U.S.'s national interests remains underexplored and undertheorized. This Note begins to bridge this gap by focusing on a particularly strong state interest: national security, as exemplified by the export controls states use in order to inhibit the extraterritorial spread of technologies and information that could be harmful to its institutions or citizens.

A complex regime of export control regulations has traditionally governed the assessment and control of national security risks as they relate to software. By definition, such controls are aimed at governing the export of software and hardware developed in the U.S. and sold or otherwise given to foreigners. In practice, they generally take the form of detailed and ever-changing lists of technical parts and sub-parts managed by United States government agencies.

The grip of software export controls has significantly loosened over the years, however. Moreover, as a growing portion of software and encryption is developed in an open source fashion—meaning publicly and collaboratively with few restrictions on further use and distribution—the regulatory hold has become even looser due to certain built-in exemptions in export controls. This trend stands in stark contrast to the overall trajectory of internet regulation in recent years.

Investigating the discrepancy between the decline in software regulation—especially in the context of open source software—versus the increase in internet regulation can shed light on different governmental approaches to the internet's challenges. A contemporary reex-

---

https://time.com/5952630/facebook-regulation-agency/ (detailing a proposal by former regulators to found a new federal agency focused exclusively on regulating digital platforms); Lina Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 790–91 (2017) (describing Amazon's market dominance and its implications with respect to antitrust law, and exploring common carrier-type regulations or stricter antitrust rules as possible responses); Dipayan Ghosh, *Are We Entering a New Era of Social Media Regulation?*, HARV. BUS. REV. (Jan. 14, 2021), https://hbr.org/2021/01/are-we-entering-a-new-era-of-social-media-regulation (exploring relevant differences between social media and traditional media platform, necessitating different regulatory approaches to each); Daphne Keller, *Platform Content Regulation – Some Models and Their Problems*, CTR. FOR INTERNET & SOC: BLOG (May 6, 2019), http://cyberlaw.stanford.edu/blog/2019/05/platform-content-regulation-%E2%80%93-some-models-and-their-problems (offering an overview of suggested models for the regulation of content on digital platforms).

6. *See generally* Paul Ohm & Blake Reid, *Regulating Software When Everything Has Software*, 84 GEO. WASH. L. REV. 1672, 1682 (2016).

amination of the state of export controls over software, and especially over free and open source software (FOSS),[7] can therefore help in mapping out the responses generated by national security interests, in particular. This exercise can then support two broader explanatory avenues: first, it explains some of the difficulties of regulating many modern software products generally, not only in the national security context. Second, it allows for a reappraisal of export controls as the correct framework for protecting national security concerns in FOSS development.

The Note proceeds as follows. After the introduction in Part I, Part II supplies a short explanation of the meaning of the term "free and open source software" and its applications in modern software development. This Part also identifies some of the challenges FOSS poses to regulatory frameworks.

Part III then turns to the question of whether the government can use tools drawn from administrative law to control FOSS endeavors, and examines the relevant U.S. regulatory framework as it is applied today through the export controls administered by the Department of Commerce, the Department of State, and the Treasury Department. The intricate and often confusing latticework of rules and implementations has by and large allowed for the unrestricted development of FOSS through a public availability exemption, found in many of the controls. Nevertheless, the government has retained some important mechanisms that could potentially constrain FOSS proliferation. Part III focuses on some of these constraints, particularly in the realms of FOSS-based encryption and FOSS monetization. It then explores the

7. There is some disagreement about the differences between "free" and "open source" software and, by extension, their corollary licenses. For some, there is a strong philosophical disagreement between those who choose to adopt "free software" and those who choose "open source software." This disagreement is sometimes extrapolated to mean that those who talk about free software mean software that is licensed under a copyleft license (usually associated with the Free Software Foundation, and discussed in II.A. *infra*), while those who use the term "open source software" mean software that is licensed under more "permissive" licenses which nevertheless abide by a list of requirements (usually associated with the Open Source Initiative). There is no need to make a conclusive decision regarding the "correct" term for the purposes of examining the impact of export controls on software, which is why the term "free and open source software" (FOSS) is used throughout (another common variation of the term is free/libre and open source software – FLOSS or F/LOSS). When discussing specific types of licenses, reference will be made to their particular requirements, and especially to the presence or absence of a "copyleft" requirement. For further elaboration on this matter, see Richard Stallman, *Why Open Source Misses the Point of Free Software*, GNU PROJECT, https://www.gnu.org/philosophy/open-source-misses-the-point.html (last updated Jan. 7, 2020); *Frequently Answered Questions: What Is "Free Software" and Is It the Same as "Open Source"?*, OPEN SOURCE INITIATIVE, https://opensource.org/faq (last visited Jan. 12, 2020).

government's ability to intervene regulatorily, building on the particular attributes of FOSS detailed in Part II. Part III shows the significant limitations and relative ambiguity of U.S. governmental controls on FOSS exports and serves as a case study of the ways in which regulators have attempted to grapple with FOSS more generally.

Part IV argues that the current U.S. export control framework does not adequately address certain risks to national security. This Part also briefly looks at some alternative approaches to regulating FOSS that the U.S. government currently pursues or could potentially pursue. Specifically, it argues that the difficulty in regulating software, and FOSS in particular, is one of the reasons administrative agencies have turned towards data regulation instead.

The study of the regulation of FOSS is, in many ways, a study of the evolution of cyber regulation. As successive generations struggle to harness the power of networked digital technologies while mitigating their destructive effects, the ways in which the law and these technologies construct and inform one another become clearer. By focusing on the export control framework and its treatment of FOSS, this Note sheds light on an especially technical but impactful part of this larger picture. The lessons of regulatory struggle and displacement elaborated herein affect the future of internet regulation and its potential to serve a multitude of important societal interests.

Ultimately, this Note does not argue for stronger export restrictions on FOSS. Others have powerfully argued elsewhere for the many advantages of allowing FOSS to continue to be borderless and collaborative.[8] Instead, this Note shows that the current regulation does not comprehensively control FOSS and tries to tease out the implications of this regulatory approach. In particular, the Note explores apparent regulatory inconsistencies when export controls are applied to particular areas of FOSS. These inconsistencies are prompting regulators to move toward data regulation as an alternative to software regulation. Tracing the causes of this displacement allows for a deeper examination of the nuanced ways in which FOSS has altered the form and function of export controls and the ways these have altered the development of FOSS in turn. The interaction between these two facets of the digital age offers a case study in how cyber governance and the

8. *See generally* YOCHAI BENKLER, THE WEALTH OF NETWORKS 13–15, 63–67, 320–23, 436–37 (2006); SAMIR CHOPRA & SCOTT DEXTER, DECODING LIBERATION: THE PROMISE OF FREE AND OPEN SOURCE SOFTWARE (2007) (presenting various arguments for FOSS's liberatory potential in culture, science, and politics); ERIC RAYMOND, THE CATHEDRAL AND THE BAZAAR (1999) (advancing an argument for public collaboration in FOSS development as the basis for better code).

internet interplay and construct one another. Understanding this dynamic is key to developing a more holistic understanding of the regulatory landscape of cyberspace.

II.
FOSS's Challenge to Regulators

FOSS is at the center of many digital infrastructures, including the internet.[9] Software developers, cybersecurity companies, start-ups, app developers, and others in the private sector, as well as governmental actors and NGOs increasingly rely on a broad range of FOSS-based products and processes.[10] As such, FOSS constitutes a core component of what cyber governance seeks to regulate.

It is therefore puzzling that export controls, a key regulatory framework, fail to properly grapple with FOSS. A deeper look shows that FOSS's pervasiveness in the economy has prompted a clash between governmental security interests and the competitive international marketplace in which American companies operate.[11] The regulatory difficulty stems from FOSS's key defining attributes, which include collaborative development and public availability with few restrictions.[12]

---

9. Nadia Eghbal, Roads and Bridges: The Unseen Labor Behind Our Digital Infrastructure 19–22, https://www.fordfoundation.org/media/2976/roads-and-bridges-the-unseen-labor-behind-our-digital-infrastructure.pdf (last visited May 30, 2021).

10. An early study characterized the growth of FOSS projects as "exponential". *See* Amit Deshpande & Dirk Riehle, *The Total Growth of Open Source*, *in* Proc. of the Fourth Conf. on Open Source Sys. 197 (2008).

11. For a historical perspective on this tension, see Robert Kuttner, *How 'National Security' Hurts National Competitiveness*, Harv. Bus. Rev., Jan.–Feb. 1991, https://hbr.org/1991/01/how-national-security-hurts-national-competitiveness. For a more contemporary appraisal of the tension as it plays out with regards to emerging and foundational technologies, see Stephen Ezell & Caleb Foote, Info. Tech & Innovation Found., How Stringent Export Controls on Emerging Technologies Would Harm the U.S. Economy (2019), http://www2.itif.org/2019-export-controls.pdf.

12. Although reference will be made throughout to FOSS as being "in the public domain", this is not strictly correct in the sense that something which is under a copyright license, as all FOSS is by definition, is not in the public domain in the same way that, for example, a work of fiction which has exceeded the time set aside for its copyrightability is then "released" into the public domain. FOSS licenses still carry terms of use that are theoretically enforceable in court, unlike the above-mentioned piece of fiction. There are types of software which are completely in the public domain by design, usually designated with a waiver of some kind. These are not the focus of the present Note because most developments in "public domain" software (in the broader sense) are built using FOSS. This is the result of a shift in the legal landscape that required an explicit statement that a piece of software was to be put in the public domain. Correspondingly, the FOSS movement gained steam in the late

This Part will supply the necessary background on FOSS and explain the difficulties encountered by regulators in their attempts to govern its development, in a general context and through export controls in particular. Through an analysis of FOSS's baked-in regulatory challenges, this Part contributes to the discussion of the historical development of export controls and other regulatory channels and the way they have responded to modern technology-driven challenges.

A. A Working Definition

In order to elucidate the difficulties of regulating FOSS, a brief sketch of some relevant concepts and working definitions is necessary. A full history of the development and proliferation of FOSS is beyond the scope of this Note and has already been extensively written about elsewhere.[13] However, this section lays out some of the basic tenets of FOSS along with several practical implications of its attributes.

From a conceptual point of view, FOSS is, according to one dominant definition, "an approach to software development that is based on shared effort on a nonproprietary model."[14] Many individuals collaborate to contribute to the development of software projects, "without any single person or entity asserting rights to exclude either from the contributed components or from the resulting whole."[15]

1980s and early 1990s. The use of FOSS over public domain continues to this day as can be seen, for example, in the number of projects hosted under each licensing regime on the software repository SourceForge, https://sourceforge.net/ (last visited Jan. 10, 2020): 128,814 under the OSI-approved open source category and only 5,353 under the public domain category. Nevertheless, most of the implications discussed below also apply to "strictly" public domain software. The terms are used synonymously here because the language in much of the regulatory material refers to the public domain, although it is often taken to include FOSS. For a discussion of the differences between FOSS licenses and the public domain, see Anupam Chander & Madhavi Sunder, *The Romance of the Public Domain*, 92 CAL. L. REV. 1331, 1358–61 (2004).

13. *See* Benkler, *supra* note 8, at 63–67; Brian W. Carver, *Share and Share Alike: Understanding and Enforcing Open Source and Free Software Licenses*, 20 BERKELEY TECH. L.J. 443 (2005); Richard Kemp, *Current Developments in Open Source Software*, 25 COMPUT. L. & SEC. REV. 569 (2009); STEVEN WEBER, THE SUCCESS OF OPEN SOURCE 20–53 (2004).

14. Benkler, *supra* note 8, at 63. Importantly, this definition somewhat minimizes the outsized influence project managers and founders often have on the development of FOSS, even if their control is not exerted through legal means (a phenomenon sometimes described as a "benign dictatorships"). For an explanation of the term in the context of FOSS projects, see Mark Federman, *The Penguinist Discourse: A Critical Application of Open Source Software Project Management to Organization Development*, 24 ORG. DEV. J. 89, 93 (2006).

15. Benkler, *supra* note 8, at 63.

In practical terms, this concept finds its translation in a particular legal licensing scheme whose main attributes are:

1. Licensing pursuant to copyright: FOSS products are copyrighted and distributed with a particular license detailing the terms of use.
2. Guarantee of free distribution: no licensing fees may be charged for software licensed under FOSS licenses.
3. Source code availability: the source code must be distributed along with the product.
4. Allowance for modifications and derivative works: the license grants users of FOSS the ability to modify the source code, which then allows them to create derivative software, or to use parts of the licensed source code in other products.
5. No discrimination: the license requires that no prohibition be placed on use by specific persons, groups, or fields of endeavor.[16]

The fundamental licensing attributes guarantee the free distribution and use of FOSS, but they are also flexible enough to allow for a variety of different licenses. Most differences in how FOSS is licensed do not affect the main goal of FOSS, or how export controls treat FOSS. However, a particular categorical divergence in licenses may affect how the regulatory framework applies to certain derivative products. There are two FOSS licensing categories that highlight this issue. The first such category encompasses licenses which include a "copyleft" clause requiring all derivative works to also be licensed under a copyleft license.[17] In this way, copyleft licenses ensure that any derivative work, even if it only includes a small portion of the

16. This list is adapted from Stephanos Androutsellis-Theotokis, Diomidis Spinellis, Maria Kechagia & Georgios Gousios, *Open Source Software: A Survey from 10,000 Feet*, 4 FOUNDS. & TRENDS IN TECH. INFO. & OPERATIONS MGMT. 187, 192–93 (2010). See also the definitions of the Free Software Foundation and of the Open Source Initiative which appear to agree on these points: *The Open Source Definition*, OPEN SOURCE INITIATIVE, https://opensource.org/docs/osd (last modified Mar. 22, 2007); *What is Free Software?*, GNU PROJECT, https://www.gnu.org/philosophy/free-sw.html (last updated Jul. 30, 2019); *Categories of Free and Nonfree Software*, GNU PROJECT, https://www.gnu.org/philosophy/categories.en.html (last updated Feb. 21, 2019). *See also* Cristina Gacek, Tony Lawrie & Budi Arief, *The Many Meanings of Open Source*, 24 IEEE SOFTWARE 34, 35–36 (2004).

17. "Copyleft" is a play on the term copyright and is intended to highlight an important divergence from the copyright mechanism in that it explicitly seeks to avoid commercialization and privatization. For further elaboration, see Richard Stallman, *The GNU Operating System and the Free Software Movement, in* OPEN SOURCES: VOICES FROM THE OPEN SOURCE REVOLUTION 53–70 (Chris DiBona, Sam Ockman & Mark Stone eds., 1999).

original source code, cannot become proprietary. The other category of licenses, sometimes called "permissive," allows for derivative works to become proprietary.[18]

From the point of view of export regulations, the divergence between copyleft and permissive FOSS licenses makes no difference in the application of regulation to software categorized as FOSS.[19] As will be discussed below, the fulcrum of the export control regulatory mechanism rests on the publication status of the relevant software. No matter how they are licensed, FOSS projects are published in similar ways, and the controls apply to them equally. Derivative software, if it becomes proprietary, can no longer be categorized as FOSS, and consequently falls outside the scope of this Note. Therefore, the rest of this Note will proceed by grouping FOSS licenses together for the purpose of analyzing the impact of export controls on FOSS.

Scholars working in the field of law and technology generally view the FOSS model as an advance of the internet age allowing for better and more secure software.[20] In an early legal exploration of the topic, Yochai Benkler pointed to the enterprise as a prominent example of "commons-based peer production" and heralded its advantages over traditional business models and market structures.[21] In recent

18. For an overview of popular licenses and the differences between them, see Kemp, *supra* note 13, 572–74; Carver, *supra* note 13; Yi-Hsuan Lin, Tung-Mei Ko, Tyng-Ruey Chuang & Kwei-Jay Lin, *Open Source Licenses and the Creative Commons Framework: License Selection and Comparison*, 22 J. INFO. SCI. & ENG'G 1 (2006); Juho Lindman, Matti Rossi & Anna Paajanen, *Matching Open Source Software License with Corresponding Business Models*, 28 IEEE SOFTWARE 31, 32 (2011).

19. The choice of license may, however, impact the success or failure of a particular project, with copyleft licenses proving to be a deterrent for the adoption of a project by developers. *See* Ravi Sen, Siddhartha S. Singh & Sharad Borle, *Open Source Software Success: Measures and Analysis*, 52 DECISION SUPPORT SYS. 364, 371 (2012) (finding "that OSS projects with semi-restrictive licenses experience a decrease in the number of subscribers and attract fewer developers"); Josh Lerner & Jean Tirole, *The Scope of Open Source Licensing*, 21 J. L. ECON. & ORG. 20, 55 (2005) (finding that "projects with less restrictive licenses tend to attract more contributors," though the authors caution that this may have something to do with the *type* of project which is usually assigned a less restrictive license); Chandrasekar Subramaniam, Ravi Sen & Matthew L. Nelson, *Determinants of Open Source Software Project Success: A Longitudinal Study*, 46 DECISION SUPPORT SYS. 576, 583 (2009) (finding "that restrictive licenses (Strong-Copyleft and Weak-Copyleft licenses) negatively impact the activity levels of the OSS project," although "Strong-Copyleft license has a negative impact *only if the target audiences are software developers*").

20. *See* Jeffrey S. Norris, *Mission-Critical Development in Open Source Software: Lessons Learned*, 21(1) IEEE SOFTWARE 42, 43 (2004); Raymond, *supra* note 8, at ch. 2.

21. Yochai Benkler, *Coase's Penguin, or, Linux and The Nature of the Firm,* 112 YALE L. J. 369, 375 (2002).

years, more and more companies that traditionally relied on proprietary software, such as Microsoft, have begun to heavily invest in FOSS and to incorporate its products into their own.[22]

One reason for this shift is FOSS's many potential applications in software development, with its uses ranging from operating systems to machine learning software.[23] Other uses prove to be impressively malleable: it can serve as "ready-made" software as a service (SaaS),[24] such as WordPress; as software development kits (SDK) which can facilitate the creation of applications and interfaces between applications; or in a variety of other ways.[25]

As a result, FOSS has become a progressively dominant component of software development. In several industries, FOSS has become the norm,[26] and its widespread adoption seems to have reached a tipping point.[27] As the next section details, this may make FOSS even

22. SYNOPSYS CYBERSECURITY RESEARCH CENTER, 2019 OPEN SOURCE SECURITY AND RISK ANALYSIS (Apr. 22, 2019) [hereinafter SYNOPSYS REPORT]. For particular examples of increased involvement and investment in FOSS, see, for example, Tom Warren, *Microsoft: We Were Wrong About Open Source*, VERGE (May 18, 2020), https://www.theverge.com/2020/5/18/21262103/microsoft-open-source-linux-history-wrong-statement; Romain Dillet, *Apple Open-Sourced the Kernel of iOS and macOS for ARM Processors*, TECHCRUNCH (Oct. 1, 2017), https://techcrunch.com/2017/10/01/apple-open-sourced-the-kernel-of-ios-and-macos-for-arm-processors/ [https://perma.cc/9KAV-N9CZ]; Swapnil Bhartiya, *How Google Uses and Contributes to Open Source*, LINUX.COM (Sep. 8, 2016), https://www.linux.com/news/how-google-uses-and-contributes-open-source/ [https://perma.cc/E3CP-W9WP].

23. *See, e.g.*, *PureDarwin*, GITHUB, https://github.com/PureDarwin/PureDarwin [https://perma.cc/6EQL-2UZN] (last visited May 29, 2021) (a FOSS operating system that forms the basis for Apple's OS X); *DeepFaceLab,* GITHUB, https://github.com/iperov/DeepFaceLab [https://perma.cc/AQ4X-2Z7W] (last visited May 29, 2021) (FOSS for creating deepfakes, which utilizes machine learning).

24. For more information on SaaS, see Dan Ma, *The Business Model of "Software-as-a-Service"*, *in* PROCEEDINGS OF THE IEEE INTERNATIONAL CONFERENCE ON SERVICES COMPUTING 701 (2007). According to Ma, "SaaS vendors offer a bundle of software applications, an IT infrastructure, and all necessary support services to users across a network. Under the SaaS business model, the software system and users' data are stored off-site in a central location run by the vendor. The vendor is in charge of all IT support services, including daily software maintenance, data backups, software upgrades, and security. Therefore, it is delivering computing utility, rather than the software only." *Id*. at 701.

25. For an analysis of several FOSS case studies, see Michael J. Gallivan, *Striking a Balance Between Trust and Control in a Virtual Organization: A Content Analysis of Open Source Software Case Studies*, 11 INFO. SYS. J. 277 (2001).

26. According to the Synopsys Report, *supra* note 22, based on data collected during auditing of commercial codebases, industries which have more FOSS than proprietary code include marketing tech, internet and mobile apps, cybersecurity, and health tech.

27. *See* Kemp, *supra* note 13; RED HAT, THE STATE OF ENTERPRISE OPEN SOURCE (2020), https://www.redhat.com/cms/managed-files/rh-enterprise-open-source-report-detail-f21756-202002-en.pdf [https://perma.cc/N5DG-SKVL]; DIGITALOCEAN, CUR-

more difficult to regulate through export controls than when its use was limited.

B. The Challenges of FOSS

Difficulties regulating FOSS stem from, among other things, the fact that cyber regulation and its subjects interplay and construct one another. The regulatory mechanism (here, export controls) and the regulatory subject (here, FOSS) alter in response to the challenges posed by the other, allowing for new permutations and applications of each. This section gives a brief overview of one side of this equation, namely, the challenges that FOSS poses to regulatory norms and to export controls. It also highlights how the First Amendment further limits regulatory efforts to control software.

FOSS's inherent openness challenges regulatory oversight in general and export controls in particular. Much of the challenge to public governance norms comes from the use of FOSS in the construction of internet architecture, which, as Lawrence Lessig famously argued, checks the government's ability to set standards.[28] According to Lessig, "[o]pen code means open control—there is control, but the user is aware of it."[29] This awareness allows for resistance, at least by the community of developers able to read and interpret software code, against the imposition of certain regulatory measures by the government.[30]

In general terms, FOSS is challenging precisely because of its dispersed and collaborative nature. Lessig argues that, in order to regulate FOSS, the government has to target not only the creator of the software, but also every other user who has a copy of the source code. In line with this reasoning, even a narrow community of developers can function as an effective—if partial—check against governmental overreach. According to this view, FOSS is not ungovernable. Rather, its essential attributes require a different kind of regulation—a shift in

---

RENTS: OPEN SOURCE 2019 (2019), https://currents.nyc3.cdn.digitaloceanspaces.com/DigitalOcean-Currents-Q4-2019.pdf [https://perma.cc/KJV9-FFHB]. Additionally, according to *The Open Source Survey*, GITHUB (2017), https://opensourcesurvey.org/2017/ [https://perma.cc/M6L2-J8VE], "[m]ost [employed respondents] report that their employers accept or encourage use of open source applications (82%) and dependencies in their code base (84%)."

28. Lawrence Lessig, *Open Code and Open Societies: Values of Internet Governance*, 74 CHI.-KENT L. REV. 1405, 1411–13 (1999).

29. LAWRENCE LESSIG, CODE: VERSION 2.0 151 (2006).

30. *Id.* There are significant limitations to relying on a community of developers in this way, both practically and ethically, but Lessig's point stands with regards to government regulations generally.

framework. In Lessig's words, "[r]egulability is conditional on the character of the code, and open code changes that character. It is a limit on government's power to regulate—not necessarily by defeating the power to regulate, but by changing it."[31]

The tension between governance and FOSS is particularly clear in the case of export controls. Centered on national security and foreign policy interests, controls over software have traditionally attempted to balance between potential threats to the state's interests and the economic value derived from the relevant exports, mostly concentrated in the American tech sector.[32] In FOSS, however, the economic value is inherently tied to its public development and availability on the internet. Regulators therefore cannot easily limit its availability without also undermining one of the chief features driving its economic value. For this reason, attempts to harden existing restrictions are often met with significant pushback from the private sector.[33]

The regulation of FOSS is further complicated because it is not always easy to identify the ways in which FOSS threatens national security. As discussed throughout the rest of the Note, these are potentially infinite, and include the 3-D printing of guns, drone operation, encryption, and other widespread cybersecurity features. The export control framework generally treats items with this range of use as "dual-use" items, that is, items for civilian or military use, which require an exporting license under certain circumstances. In the case of FOSS, however, many products remain entirely outside the purview of export regulations, even when they are practically identical to proprietary products which are regulated.

Finally, in addition to ways in which FOSS tests regulatory norms and export controls, regulators are limited by the First Amend-

---

31. *Id.* at 152–53.

32. *See, e.g., Export Controls, Arms Sales, and Reform: Balancing U.S. Interests, Part 1: Hearing Before the H. Comm. on Foreign Affs.*, 112th Cong. 1 (2011) (Statement of Rep. Ileana Ros-Lehtinen, Chairman, H. Comm. on Foreign Affs.) ("United States policy, with respect to the export of sensitive technology, has long been to seek a balance between the U.S. economic interest in promoting exports, and our national security interest in maintaining a military advantage over potential adversaries, and denying the spread of technologies that could be used in developing weapons of mass destruction.").

33. For a contemporary example of this dynamic, see Cade Metz, *Curbs on AI Exports? Silicon Valley Fears Losing Its Edge*, N.Y. TIMES (Jan. 1, 2019), https://www.nytimes.com/2019/01/01/technology/artificial-intelligence-export-restrictions.html [https://perma.cc/5RRX-ESVG]. A similar dynamic emerged during the export control debate over cryptography in the 1990s, with civil society groups joining technology firms to oppose several restrictive bills. *See generally* STEVEN LEVY, CRYPTO: HOW THE CODE REBELS BEAT THE GOVERNMENT – SAVING PRIVACY IN THE DIGITAL AGE (2002).

ment. Since courts have sometimes recognized software as speech,[34] the U.S. government's ability to regulate source code is at least somewhat limited by the Constitution. In fact, the tension between national security interests and free speech has in the past been a significant factor leading to the loosening of export controls on encryption.[35] Software and code are not the only areas in which First Amendment interpretation has expanded significantly in the last few decades, but they do force other regulatory tools of the state to stretch in response to assertions of code as speech.[36] This can lead to increasingly incongruous regulatory interpretations, such as the claim, discussed in more detail in Part III below, that the internet is alternately part of and not part of the public domain.

While collaborative peer production may not have led to the overarching freedom-promoting effects early theorizers advanced,[37] export controls in particular have changed at least in part as a result of the way FOSS is created and developed. As argued in Parts III and IV, the export controls regulatory framework has been unable to adapt in response to FOSS challenges highlighted in this section and have therefore become ineffective. The resulting regulatory alterations may help to explain some of the attempts to displace software regulation with data regulation, as explored below.

---

34. The most relevant cases in which this proposition has been discussed directly are *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000); *Bernstein v. U.S. Dep't of State*, 922 F. Supp. 1426 (N.D. Cal. 1996), *aff'd sub nom.* Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132 (9th Cir. 1999), *withdrawn and reh'g granted*, 192 F.3d 1308 (1999). For a discussion of the debate on this topic see, for example, Jorge R. Riog, *Decoding First Amendment Coverage of Computer Source Code in the Age of YouTube, Facebook, and the Arab Spring*, 68 N.Y.U. ANN. SURV. AM. L. 319 (2012); Kyle Langvardt, *The Doctrinal Toll of "Information as Speech"*, 47 LOY. U. CHI. L.J. 761 (2016); Ryan Christopher Fox, *Old Law and New Technology: The Problem of Computer Source Code and the First Amendment*, 49 UCLA L. REV. 871, 887–88 (2002); Robert Post, *Encryption Source Code and the First Amendment*, 15 BERKELEY TECH. L.J. 713 (2000); Lee Tien, *Publishing Software as a Speech Act*, 15 BERKELEY TECH. L.J. 629 (2000); Orin S. Kerr, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 WASH. & LEE L. REV. 1287 (2000).

35. Christopher F. Corr, *The Wall Still Stands! Complying with Export Controls on Technology Transfers in the Post-Cold War, Post-9/11 Era*, 25 HOUSTON J. INT'L L. 441, 485–87 (2003); Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 439–40 (2011).

36. The link between speech and code in the context of export controls is complex and is not developed fully here. For an interesting treatment which delves further into the connection between speech, particularly dangerous speech, and the regulation of dual-use items through export controls, see Eugene Volokh, *Crime-Facilitating Speech*, 57 STAN. L. REV. 1095, 1107–27 (2005).

37. Cohen, *supra* note 4, at 251–54.

III.
SOFTWARE EXPORT RESTRICTIONS AND FOSS

FOSS's attributes are but one side of a complex interaction. On the other side are export controls, whose purpose is to protect vital national security and foreign policy interests of the state.[38] These are very broad (perhaps overbroad) categories, but in the context of technology and software, they generally encompass the regulation of items with an exclusively military purpose, as well as dual-use items,[39] which have both civilian and military purposes. In many ways, export controls function as a categorization mechanism, sorting the world into threatening technologies that require strict regulation and non-threatening technologies that require only lax oversight, or none at all. This is sometimes a nuanced process. For example, the M1 Abrams Tank used by the U.S. Army is regulated as a military item by export controls,[40] but some of its individual parts, such as its brake components, can be regulated as dual-purpose items.[41]

In the past, export restrictions focused mainly on arms and dual-use machinery as part of a Cold War effort to withhold U.S.-developed technology with potentially military applications from the U.S.S.R.[42] In recent decades, as regulations broadened to accommodate new threats posed by terrorism and facilitated by the internet, regulators have increasingly turned their attention to software and encryption.[43]

---

38. JOHN R. LIEBMAN, ROSZEL C. THOMSEN II, JAMES E. BARTLETT III & JOHN C. PISA-RELLI, UNITED STATES EXPORT CONTROLS 1–2 (7th ed. 2019).

39. The relevant regulatory framework does not contain a precise definition of what constitutes an "item", and various terms are used to delineate the scope of products, commodities and technologies which fall within the jurisdiction of the various regimes. I have attempted to provide precise definitions where this was possible, but the regulations themselves are rather vague about itemization in the abstract, and seem to rely on a general understanding, best described in the EAR, of items as "commodities, software and technology." 15 C.F.R. § 772.1 (2021).

40. *Id.* at Category VII(a)(1).

41. *Id.* at Category VII(g); 15 C.F.R. § 774 (Supp. I 2021) at ECCN 0A606.y.

42. LIEBMAN ET AL., *supra* note 38.

43. See Fabian Bohnenberger, *The Proliferation of Cyber-Surveillance Technologies: Challenges and Prospects for Strengthened Export Controls*, 3 STRATEGIC TRADE REV. 81 (2017) and Ben Wagner & Stéphanie Horth, *Digital Technologies, Human Rights and Global Trade? Expanding Export Controls of Surveillance Technologies in Europe, China and India*, *in* RESEARCH HANDBOOK ON HUMAN RIGHTS AND DIGITAL TECHNOLOGY (Ben Wagner, Matthias C. Kettemann, & Killian Vieth eds., 2019) for a discussion of expanding controls on surveillance technologies, including software. Similarly, see Chad P. Bown, *Export Controls: America's Other National Security Threat*, 30 DUKE J. COMPAR. & INT'L L. 283 (2020) for a discussion of the Trump administration's strengthening of controls on AI exports.

The expansion in export controls also led to an increase in the number of regulatory agencies engaged in export regulations.[44] An Obama-era review of export controls was emblematic of the criticism generally levelled at this expansion, concluding that the export controls framework is "overly complicated, contains too many redundancies, and tries to protect too much."[45] The result of this review, the National Export Initiative, constitutes an attempt to harmonize the relevant regulations and agencies. In practice, changes to the regulatory framework have been slow, and the number of regulators handling exports remains large.[46]

Following the general description of FOSS and its challenges laid out in Part II, this Part argues that current controls are not well-tailored for the changes in software development brought about by the explosion in the use of FOSS. The sections below briefly describe the relevant U.S. export controls as they relate to software and sketch their role in accomplishing the overarching goal of export regulations.[47] The last section explores the ways in which export controls, despite their general failure to regulate FOSS, may nevertheless intervene in its development. These interventions affect mostly the periphery of FOSS development, but they serve to highlight the fact that export controls are not entirely toothless.

A. U.S. Export Restrictions on Software

The export control regulatory framework includes several different administrative bodies and a messy latticework of legislation. In tracing this landscape and its operations, this section investigates the intricate ways in which FOSS eludes most export control regulatory hooks. The focus here is on the main regulatory bodies exerting an influence on FOSS, including the Bureau of Industry and Security, the Office of Foreign Assets Control and the Directorate of Defense Trade Controls.

These regulators derive power from the relatively wide array of sanctions they can enforce against violators. Generally, if a regulation applies to a particular exported product, the exporter must seek a li-

44. In 2010, President Obama issued Executive Order Number 13,558, 3 C.F.R. § 271 (2011), establishing the Export Enforcement Coordination Center (E2C2), which includes representative from eight governmental departments and 18 federal agencies.

45. PRESIDENTIAL STUDY DIRECTIVE 8 (Dec. 21, 2009).

46. LIEBMAN ET AL., *supra* note 38, at § 1.05.

47. This list is not exhaustive. For example, it does not focus on additional measures the U.S. employs, such as the Committee on Foreign Investment in the United States (CFIUS), although these will be briefly discussed in Part IV, *infra*.

cense from the relevant agency (or agencies), unless a general license requiring no pre-approval is available. The possible sanctions for violations are severe and include hefty fines, the seizure of goods and assets, denial of exporting and contracting entitlements, and, in certain cases, imprisonment.[48] As explored below, FOSS is not usually subject to any of these because of its frequent wholesale exemption from controls.

i. Export Administration Regulations and the Bureau of Industry and Security

Mapping FOSS's exclusion from the purview of export controls requires familiarity with some important details of said controls. This section details the operations of the Bureau of Industry and Security (BIS), starting with its classification of regulable software and the ways in which FOSS is carved out of that definition through a "public availability" exemption which essentially leaves FOSS entirely outside the purview of Export Administration Regulation controls. It then explores the Export Control Reform Act (ECRA), which may grant the BIS power to claw back some control over FOSS. It remains unclear how the BIS will ultimately craft its regulations in light of this legislation, but, at least for the moment, its efforts appear to leave FOSS mostly untouched.

Situated within the Department of Commerce, the BIS administers the Export Administration Regulations (EAR), a complex array of controls implementing the Export Control Reform Act,[49] which itself repealed and replaced the Export Administration Act of 1979.[50] The BIS's mission statement elaborates on the purpose of these controls: to "[a]dvance U.S. national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership."[51] Export authorization in specific cases depends on the nature of the exported product, its end use, the target country, and the intended end user.[52]

The EAR framework, like many other export controls, is premised on technically detailed definitions and sub-definitions, creating

48. LIEBMAN ET AL., *supra* note 38.

49. For a deeper overview of the relevant legislation, see Corr, *supra* note 35.

50. IAN F. FERGUSON & PAUL K. KERR, CONG. RSCH. SERV., R41916, THE U.S. EXPORT CONTROL SYSTEM AND THE EXPORT CONTROL REFORM INITIATIVE 2 (2020).

51. *Mission Statement*, BUREAU OF INDUSTRY AND SECURITY, https://www.bis.doc.gov/index.php/about-bis/mission-statement (last visited May 28, 2021).

52. 15 C.F.R. §§ 744.1-20 (2021).

an unwieldy maze of categories, governed by the Commerce Control List (CCL). The CCL categorizes items with both civilian and military uses—called dual-use items[53]—that are subject to export restrictions.[54] The detailed manner in which the EAR approaches the regulation of most dual-use items stands in stark contrast to the hands-off approach FOSS receives. The EAR distinguishes between "item," which it defines as "commodities, software and technology,"[55] and "software," which it defines as "a collection of one or more 'programs' [meaning "a sequence of instructions to carry out a process in, or convertible into, a form executable by an electronic computer"] or 'microprograms' fixed in any tangible medium of expression."[56] Meanwhile, "technology" is defined—somewhat tautologically—as "information necessary for the 'development,' 'production,' 'use,' operation, installation, maintenance, repair, overhaul, or refurbishing . . . of an item."[57] The EAR places software in a context that ties it to commodities and technologies, indicating the regulator's effort to cohesively control different facets of technological innovation.

If an "item," as defined by the EAR, also falls under the jurisdiction of one of several different governmental bodies (State Depart-

53. The precise definition of "items subject to the EAR" can be found in 15 C.F.R. § 734.3:

"(1) All items in the United States, including in a U.S. Foreign Trade Zone or moving in transit through the United States from one foreign country to another;

(2) All U.S. origin items wherever located;

(3) Foreign-made commodities that incorporate controlled U.S.-origin commodities, foreign-made commodities that are 'bundled' with controlled U.S.-origin software, foreign-made software that is commingled with controlled U.S.-origin software, and foreign-made technology that is commingled with controlled U.S.-origin technology:

(i) In any quantity, as described in § 734.4(a) of this part; or

(ii) In quantities exceeding the de minimis levels, as described in § 734.4(c) or § 734.4(d) of this part;

(4) Certain foreign-made direct products of U.S. origin technology or software, as described in § 736.2(b)(3) of the EAR. The term "direct product" means the immediate product (including processes and services) produced directly by the use of technology or software; and

(5) Certain commodities produced by any plant or major component of a plant located outside the United States that is a direct product of U.S.-origin technology or software, as described in § 736.2(b)(3) of the EAR."

Moreover, 15 C.F.R. § 730.3 defines a "dual-use" item as an item that "has civil applications as well as terrorism and military or weapons of mass destruction (WMD)-related applications."

54. Although the United States regulates dual-use goods and technologies through the EAR, it is also party to the Wassenaar Arrangement, a multilateral agreement on export controls of arms and dual-use items.

55. 15 C.F.R. § 772.1 (2021).

56. *Id.*

57. *Id.*

ment, Treasury Department, Energy Department, Nuclear Regulatory Commission, or the Patent and Trademark Office), the EAR yields to the latter body's regulations.[58]

Because of their potential use in both civilian and military contexts, software and encryption products generally fall within the scope of the EAR. However, there are two important exceptions to the regulations which affect the EAR's licensing scheme (the second of which directly affects how FOSS works under the EAR). The first concerns mass market software: software that is both (a) generally available to the public because it is sold from stock without restrictions and (b) "[d]esigned for installation by the user without further substantial support by the supplier."[59] The EAR, while governing such software, allows for its export under a general license, provided the export destination is not one of the countries specifically carved out of the exception.[60]

Unlike the first exception, the second exception includes software which is completely outside the jurisdiction of the EAR—and therefore does not require a license whatsoever.[61] This category—which includes software that has been or will be published online or elsewhere, arises during or results from fundamental research, is educational, or is included in some patent applications—is fairly straightforward, although it does not apply to certain encryption software.[62] Because it is published online by definition, FOSS falls squarely within this public availability exemption, and thus wholly outside the purview of the EAR.

58. 15 C.F.R. § 734.3(b). As 15 C.F.R. § 730.3 puts it, "In essence, the EAR control any item warranting control that is not exclusively controlled for export, reexport, or transfer (in-country) by another agency of the U.S. Government or otherwise excluded from being subject to the EAR pursuant to § 734.3(b) of the EAR."

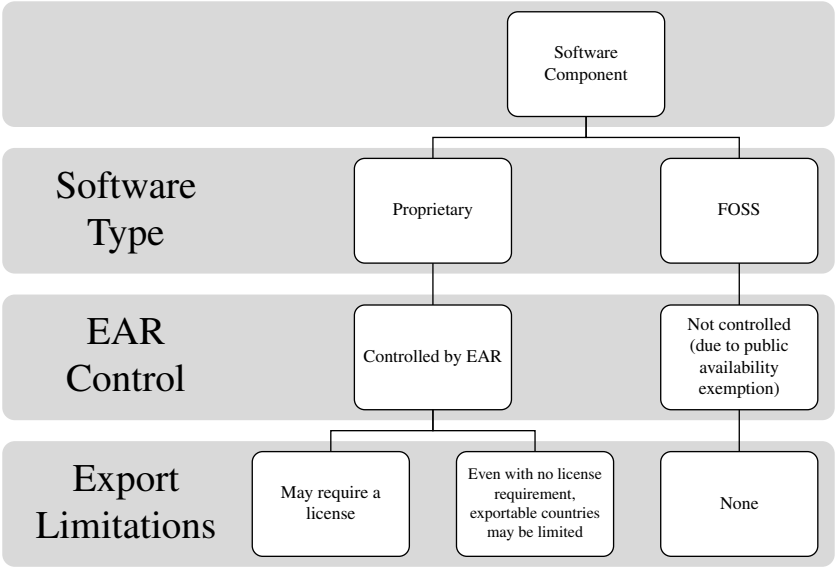
59. 15 C.F.R. §§ 740.13(d)(3)(ii)(A)–(B) (2021).

60. *Id.* at § 740.13(d). The relevant countries to which mass market export is currently unavailable are Iran, North Korea, and Syria.

61. 15 C.F.R. § 734.3(b)(3). In 2016, the BIS issued a revision of this category in order to clarify that the internet qualifies as a publishing medium. *See* Revisions to Definitions in the Export Administration Regulations, 81 Fed. Reg. 35,586 (June 3, 2016) [hereinafter 2016 Revisions].

62. Encryption software has its own public availability exemption which includes an important caveat, discussed in detail in Part III.B., *infra*.

TABLE I: EAR CONTROLS ON SOFTWARE



FOSS's wholesale exemption from EAR controls could potentially change in response to future BIS activity pursuant to the Export Control Reform Act (ECRA), which took effect on August 13, 2018.[63] Section 1758 is of particular interest for the purposes of this Note. Although the BIS already had the authority to regulate previously uncontrolled commodities, technologies, or software characterized as "emerging and foundational technologies" that are important for national security or foreign policy reasons, the new law makes identifying and controlling them a priority. The BIS has not fully defined these technologies as of yet, but, in its request for public comment about the criteria for the identification of emerging technologies, the bureau referenced artificial intelligence, data analytics technology, and quantum information and sensing technology, among others, as potential candidates.[64]

All of these technologies have roots and applications in FOSS,[65] putting the new law and its interpretation on a collision course with

63. Export Control Reform Act, 50 U.S.C.A. § 4801 (West 2018).

64. Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58,201 (proposed Nov. 19, 2018).

65. *See, e.g.*, Mark Fingerhuth, Tomáš Babej & Peter Wittek, *Open Source Software in Quantum Computing*, 13(12) PLOS ONE (2018); Sambit Bhattacharya, Bogdan Czejdo, Rajeev Agrawal, Erdem Erdemir & Balakrishna Gokaraju, *Open Source Platforms and Frameworks for Artificial Intelligence and Machine Learning* (conference paper, 2018).

preexisting regulations, and particularly with the public availability exemption. If the BIS intends to regulate any iteration of artificial intelligence, data analytics or quantum information, it will have to impose regulations on FOSS. This will, by definition, narrow the scope of the exemption FOSS currently benefits from. On the other hand, if the exemption is to retain its expansive nature, ECRA may fail to meet its declared objective of regulating emerging and foundational technologies.[66] It remains to be seen what use the BIS will make of ECRA in practice. Although the BIS has issued its rule on emerging technologies,[67] and has begun the process of identifying foundational technologies,[68] there has been no talk of withdrawing the public availability exemption.

Ultimately, the EAR maze of regulations attempts to corral the export of items, including software, with the goal of advancing U.S. national security and foreign policy interests. In the process, its framework has excluded FOSS from the purview of regulatory control, revealing an inability to formulate regulations that curb FOSS's more conspicuous threats to national security while preserving the accessibility and availability that make it valuable. The BIS's recent attempts to regulate emerging technology while ignoring the role FOSS plays in them can also be read as a tacit acknowledgement of the mismatch between its regulatory capabilities and the reality of FOSS-based technological innovation.

ii. Office of Foreign Assets Control Regulations and the Department of the Treasury

In contrast to the broad scope of the EAR, the Department of the Treasury's Office of Foreign Assets Control (OFAC) regulations are

66. Roszel C. Thomsen II, *Artificial Intelligence and Export Controls: Conceivable, but Counterproductive?*, 22 J. INTERNET L. 15, 18–19 (2018) (arguing that "[i]mposing export controls on proprietary AI software would do nothing more than favor one business model (open source) over another business model (proprietary code), unless the United States attempts to prohibit publication of open source software, with the attendant First Amendment issues looming large.").

67. Addition to Software Specially Designed to Automate the Analysis of Geospatial Imagery to the Export Control Classification Number 0Y521 Series, 85 Fed. Reg. 459 (Jan. 6, 2020). The new rule is extremely narrow in scope – it imposes license requirements on the export of software that uses neural networks to discover "points of interest" in geospatial imagery. Furthermore, the new rule only applies to software with a graphical user interface. *Id*.

68. The BIS's approach towards foundational technologies appears to be more amorphous at this point. In fact, the Bureau does not put forward categories in Identification and Review of Controls for Certain Foundational Technologies, 85 Fed. Reg. 52,934 (proposed Aug. 27, 2020). Instead, it has turned to the public and to the industry in order to begin the process of identifying the relevant technologies. *Id*.

aimed at particular countries, regions, or types of goods. OFAC handles much of the administrative activity around economic and trade sanctions and embargoes, and thus its regulations are oriented chiefly around financial transactions, pursuant to the Trading With the Enemy Act and the International Emergency Economic Powers Act.[69]

EAR and OFAC regulations have some overlap, but, as previously noted,[70] the EAR does not generally control items administered by OFAC.[71] Despite the fact that few OFAC provisions specifically address software, they may nevertheless apply to the export of software through general sanctions against particular countries. Within the ambit of specific countries, their scope is quite broad, often requiring the acquisition of a license for the export of almost any good.[72]

OFAC controls do, however, contain certain exemptions. Most relevant among these is an exemption for "information and informational materials,"[73] including "publications," which presumably contain electronically published material.[74] The relevant provisions often contain a caveat that such publications are exempt if they are not otherwise controlled for national security or foreign policy reasons[75]—criteria which generally do not apply to FOSS under EAR, as explored above, or under ITAR, explored below. Alternatively, practitioners

69. For an empirical study of OFAC's enforcement of sanctions, see Bryan R. Early & Keith A. Preble, *Going Fishing Versus Hunting Whales: Explaining Changes in How the US Enforces Economic Sanctions*, 29 SEC. STUD. 231 (2020).

70. See *supra* note 58 and accompanying text.

71. There is some ambiguity about this matter because BIS refers exporters to both agencies (BIS and OFAC) for exports to some regions covered jointly. *See* 15 C.F.R. § 746 (2021) for examples of the EAR referring to OFAC controls in overlapping jurisdictions (e.g. § 746.2(d); § 746.4(e)) and for examples in which OFAC controls suffice (e.g. § 746.7(a)(2)).

72. Lee Baker, *The Unintended Consequences of US Export Restrictions on Software and Online Services for American Foreign Policy and Human Rights,* 23 HARV. J. L. & TECH. 537, 544 (2010) (describing OFAC's broad mandate in relation to certain country-specific sanctions, citing Iran as an example: "the "exportation, reexportation, sale, or supply. . . of any goods, technology, or services to Iran," barring certain closely circumscribed exemptions, is prohibited without an OFAC license").

73. These can be found in many of the restrictions for specific countries, e.g. 31 C.F.R. § 560.210(c) (2012) [Iran]; 31 C.F.R. § 510.213(c) (2020) [North Korea]; 31 C.F.R. § 515.206(a) (2016) [Cuba], etc. These reflect the 1988 and 1994 amendments to the Trading with the Enemy Act and the International Emergency Economic Powers Act, Pub. L. No. 100-418, 102 Stat. 1371 (1988); Foreign Relations Authorization Act, Fiscal Years 1994 and 1995, Pub. L. No. 103-236, 108 Stat. 382 (1994) – the "Berman Amendments," named after Rep. Howard Berman, who introduced them.

74. BENJAMIN H. FLOWE, JR., BERLINER CORCORAN & ROWE LLP, COMPLIANCE WITH U.S. EXPORT AND REEXPORT CONTROLS, ¶ 12.6.1(a) (Nov. 2013), https://bcr.tv/ExportandReexportComplianceGuide_Master_Version_November_2013.pdf.

75. *See, e.g.*, 50 U.S.C. § 1702(b)(3) (2018).

have also argued that the regulations explicitly place technology and software regulated by the EAR outside the purview of the informational material exemption,[76] thus implying that software that is explicitly exempt from the EAR due to being publicly available is also not subject to OFAC export controls. This holds true even for software exported to embargoed countries.[77] On the other hand, OFAC sometimes specifically authorizes the export of publicly available software, perhaps as a declaratory measure.[78] It is therefore not entirely clear what the origin of the exemption is under OFAC. Regardless, however, to the author's knowledge at the time of publication of this Note, OFAC has not taken action against people who post FOSS online.

Though OFAC by and large exempts publicly available software, there is a related question regarding software-as-a-service (SaaS). Generally speaking, OFAC sanctions prohibit the export or reexport of services from the U.S. to embargoed countries or for the benefit of those countries' governments.[79] Insofar as SaaS can be conceptually separated from software, it seems likely that an extension of these obligations for a U.S.-based SaaS provider would include a prohibition on supplying this type of service to embargoed countries or to people enumerated on the list of specially designated nationals and blocked persons compiled by OFAC.[80] OFAC has partially addressed this question in several general licenses, and it appears that a differentiation is made between fee-based services and free services.[81] The impact of this differentiation on FOSS-based SaaS is explored in Section C below.

---

76. *See, e.g.*, 31 C.F.R. § 560.210(c)(3) [Iran]. Similar exemptions appear in the sanction regulations regarding other countries.

77. BENJAMIN H. FLOWE, JR., BERLINER CORCORAN & ROWE LLP, EXPORTING TECHNOLOGY AND SOFTWARE, PARTICULARLY ENCRYPTION, ¶ 1.1.1 (Oct. 2018), http://bcr.tv/Exporting_Technology_and_Software_Particularly_Encryption_2018_Final-1.pdf.

78. General License with Respect to Certain Services, Software, and Hardware Incident to Personal Communications, 78 Fed. Reg. 43,278 (July 19, 2013) [hereinafter: General License D-1].

79. Although important exemptions have been authorized, for example in relation to "fee-based services incident to the exchange of personal communications over the Internet." *Id*.

80. John F. McKenzie, *U.S. Export Controls on Internet Software Transactions*, 44 INT'L LAW. 857, 868 (2010).

81. *See* General License D-1, *supra* note 78.

iii. International Traffic in Arms Regulations and the Directorate of Defense Trade Controls

In addition to controls administered by the Treasury and Commerce Departments, the State Department's Directorate of Defense Trade Controls (DDTC) controls defense-related exports through the International Traffic in Arms Regulations (ITAR). The U.S. Munitions List (USML), detailed in Part 121 of ITAR, is a list of "articles, services and related technical data"[82] principally designed for military use (called "defense articles"), regulated under ITAR.[83] The DDTC has jurisdiction to determine questions of authority regarding dual-use items, essentially granting it the exclusive power to determine whether ITAR or the EAR applies to a particular item. The involvement of several different agencies, especially with so broad an overlap in their subject matter jurisdiction, burdens the export licensing process and causes significant friction and delay for businesses.[84] Due to these issues and to the ambiguity brought about by inter-agency infighting, several categories of items have shifted in recent years from the USML (regulated under ITAR) to the CCL (regulated under the EAR).[85]

The defense articles listed in the USML largely include military items such as munitions, tanks, and nuclear weapons. However, the list also includes items not immediately linked to military usage, such as communication and navigation satellites, and importantly, a category called "technical data."[86] The definition of "technical data," in turn, includes "software directly related to defense articles."[87] If one follows closely the nesting definitions here, the result is that "software

82. 22 C.F.R. § 121.1(a) (2020).

83. 22 C.F.R. § 120.6 gives the following definition of "defense article": "any item or technical data designated in [The USML]."

84. Corr, *supra* note 35, at 464–67.

85. For statistics regarding this shift, see the reports of the BIS's Office of Technology Evaluation: *USML to CCL Regulatory Changes*, BUREAU OF INDUS. & SEC., https://www.bis.doc.gov/index.php/statistical-reports/ecr-analysis (last visited May 24, 2021) [https://perma.cc/4XG4-PPXY].

86. 22 C.F.R. § 120.6 (2020).

87. 22 C.F.R. § 120.10(a)(4) (2020). The full definition of "technical data" is:
"(a). . .
(1) Information, other than software as defined in § 120.10(a)(4), which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation.
(2) Classified information relating to defense articles and defense services on the U.S. Munitions List and 600-series items controlled by the Commerce Control List;
(3) Information covered by an invention secrecy order; or
(4) Software (see § 120.45(f)) directly related to defense articles.

directly related to defense articles" is ambiguously defined because it appears in the definition of "defense article," and thus refers to itself in its definition. This circularity, even if not used capriciously by the DDTC, highlights the nebulous characterization assigned to software and points to the ambiguity surrounding exports. Filing a "commodity jurisdiction" request with the DDTC can partially resolve this vagueness, helping to determine whether a particular piece of software qualifies as a "defense article."[88] This process naturally entails additional bureaucratic hurdles, which can easily result in significant delays.

ITAR, like the EAR, contains an important carve-out for publicly available information in the form of an exclusion for fundamental research and information in the "public domain."[89] Pertinently, ITAR defines the public domain so that it does not automatically include any and all information available to the public. Instead, information is made publicly available in one of eight prescribed ways, which do not currently include the internet.[90]

(b) The definition in paragraph (a) of this section does not include information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities, or information in the public domain as defined in § 120.11 of this subchapter or telemetry data as defined in note 3 to Category XV(f) of part 121 of this subchapter. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles."

"Software", in contrast to the EAR's relatively clear definition, "includes but is not limited to the system functional design, logic flow, algorithms, application programs, operating systems, and support software for design, implementation, test, operation, diagnosis and repair." 22 C.F.R. § 120.45 (2014).

It is interesting to note that under the ITAR definition software qualifies as "data" of a sort, which seems to neglect an important distinction in the executability of software as opposed to data. For more on the differences, see Daniel S. Katz, Kyle e. Niemeyer, Arfon M. Smith, William L. Anderson, Carl Boettiger, Konrad Hinsen, Rob Hooft, Michael Hucka, Allen Lee, Frank Löffler, Tom Pollard & Fernando Rios, *Software vs. Data in the Context of Citation* PEERJ PREPRINTS (Dec. 10, 2016), https://peerj.com/preprints/2630v1/ [https://perma.cc/59E4-6MU8].

88. 22 C.F.R. § 120.4 (2020).

89. 22 C.F.R. § 120.11 (2020). Although the definition of "software" under ITAR does not include the word "information," the surrounding definition of "technical data" implies that software may also be a type of information (particularly paragraph (b) detailing the possible exemptions). Moreover, the proposed revisions of ITAR suggest that the DDTC considers software as potentially falling within the public availability exemption.

90. According to 22 C.F.R. § 120.11, these are:

"(1) Through sales at newsstands and bookstores;

(2) Through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information;

(3) Through second class mailing privileges granted by the U.S. Government;

(4) At libraries open to the public or from which the public can obtain documents;

(5) Through patents available at any patent office;

(6) Through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public, in the United States;

A proposed 2015 revision of ITAR would have expanded the definition of "public domain" to include publication via the internet. However, the same revision would have also added a provision according to which:

> [T]echnical data or software, whether or not developed with government funding, is not in the public domain if it has been made available to the public without authorization from: (1) The Directorate of Defense Trade Controls; (2) The Department of Defense's Office of Security Review; (3) The relevant U.S. government contracting entity with authority to allow the technical data or software to be made available to the public; or (4) Another U.S. government official with authority to allow the technical data or software to be made available to the public.[91]

Perhaps due to substantial public opposition to this latter provision for reasons outside the scope of this Note,[92] neither of these proposals has been adopted as official ITAR amendments.

---

(7) Through public release (i.e., unlimited distribution) in any form (e.g., not necessarily in published form) after approval by the cognizant U.S. government department or agency (see also § 125.4(b)(13) of this subchapter);

(8) Through fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community. Fundamental research is defined to mean basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. University research will not be considered fundamental research if:

(i) The University or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity, or

(ii) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable."

91. International Traffic in Arms: Revisions to Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions, 80 Fed. Reg. 31,525, 31534 (June 3, 2015).

92. Flowe, *supra* note 77, at ¶ 1.1.1. The proposed rule has 9986 submitted comments on the government's website www.regulations.gov, many of them opposed to the rule, for a variety of reasons. For some relevant examples, see Edward J. Ray, Comment Letter on ITAR Amendment – Revisions to Definitions; Data Transmission and Storage (Aug. 3, 2015), https://www.regulations.gov/document?D=DOS-2015-0023-7993; Intel Corp., Comment Letter on International Traffic in Arms: Revisions to Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions (Aug. 3, 2015), https://www.regulations.gov/document?D=DOS-2015-0023-7566; and J. Patrick Briscoe, Comment Letter on ITAR Amendment – Revisions to Definitions; Data Transmission and Storage (Aug. 3, 2015), https://www.regulations.gov/document?D=DOS-2015-0023-7289.

The current state of affairs therefore casts substantial doubt as to whether ITAR applies to a piece of software, even if it has no immediate military use. Furthermore, the conditions under which military-use software is *actually* exempt when it is published online remain unclear. Consequently, the DDTC possesses considerable discretion in its application of ITAR to software. In practice, however, it appears that the DDTC is mainly concerned with clear military applications, hence the gradual shift of more items from the USML to the CCL.[93]

On a more granular level, the case of *Defense Distributed v. Department of State* provides insight into the DDTC's application of ITAR's extensive definitions. Defense Distributed is an organization which develops digital blueprints of firearms in CAD files and distributes them freely online. The files are then downloaded and printed using a three-dimensional printer, resulting in the production of potentially undetectable "ghost guns." In 2013, the DDTC, citing an ITAR violation,[94] directed the organization to remove files it had published that held the blueprints for parts of a printable single-shot handgun. The case deals with the dissemination of "information," rather than software, but its lessons are applicable to the interpretation of ITAR in both cases.

In 2015, Defense Distributed, joined by the Second Amendment Foundation, filed suit against the State Department in a federal district court, arguing that the DDTC's interpretation of ITAR "constitutes an unconstitutional prior restraint on protected First Amendment speech,"[95] and violates the Second and Fifth Amendments. The district court denied the request for a preliminary injunction.[96] The Fifth Circuit Court of Appeals subsequently affirmed this ruling and the Supreme Court denied a writ of certiorari.

In its decision, the Fifth Circuit characterized Defense Distributed's appeal as a request for "a declaration that no prepublication approval is needed for privately generated unclassified information, whether or not that data may constitute 'technical data' relating to

93. Revisions to the Export Administration Regulations: Initial Implementation of Export Control Reform, 78 Fed. Reg. 22,659 (Apr. 16, 2013) (explaining that reforms shifting items from the USML to the CCL are enacted so that ITAR controls "only the items that provide the United States with a critical military or intelligence advantage or otherwise warrant such control").

94. Specifically, the DDTC's letter cites a possible violation of 22 C.F.R. § 120.10: "information, other than software as defined in § 120.10(a)(4), which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation."

95. Def. Distributed v. U.S. Dep't of State, 838 F.3d 451, 456 (5th Cir. 2016).

96. Def. Distributed v. U.S. Dep't of State, 121 F. Supp. 3d 680 (W.D. Tex. 2015).

items on the USML."[97] In its affirmation of the denial of a preliminary injunction, the court echoed the district court's holding that "the government's exceptionally strong interest in national defense and national security outweighs Plaintiffs–Appellants very strong constitutional rights under these circumstances."[98]

Although the majority sidestepped the issue, direct engagement with the DDTC's interpretation of ITAR proves how ambiguous the text is. In his dissenting opinion, Judge Jones warned against the "embedded ambiguity, and disturbing breadth, in the State Department's discretion to prevent the dissemination (without an 'export' license) of lawful, non-classified technical data to foreign persons within the U.S."[99] Moreover, he highlighted the inherent vagueness in the DDTC's argument as it relates to the public domain:

> If any dissemination of information bearing on USML technical data to foreign persons within the U.S. is potentially an 'export,' then facilitating domestic publication of such information free of charge can never satisfy the 'public domain' exception because newspapers, libraries, magazines, conferences, etc. may all be accessed by foreign persons. The State Department's *ipse dixit* that 'export' is consistent with its own 'public domain' regulation is incoherent and unreasonable. Even if these regulations are consistent, however, attempting to exclude the Internet from the 'public domain,' whose definition does not currently refer to the Internet, is irrational and absurd. The Internet has become the quintessential 'public domain.' The State Department cannot have it both ways, broadly defining 'export' to cover non-transactional publication within the U.S. while solely and arbitrarily excluding from the 'public domain' exception the Internet publication of Defense Distributed's technical data.
>
> The root of the problem is that the State Department's litigating position and its regulations put more weight on 'export' than any reasonable construction of the statute will bear.[100]

Although the case deals more directly with data (or "information") than with software, the data in question carries similar attributes to FOSS and indeed highlights the contradictions that abound when regulators attempt to force an existing framework (export controls) to fit information freely distributed online. The dispersed, public, and collaborative nature of this data, and of FOSS by extension, can only

97. *Def. Distributed*, 838 F.3d at 456.
98. *Id.* at 458.
99. *Id.* at 467.
100. *Id.* at 468.

fit promulgated export regulations through anachronistic interpretations which mandate that the internet be excluded as a venue of unconstrained publication. The facts of *Defense Distributed* serve as a critique not of the overarching state interest in limiting gun dissemination (which is easily articulated and reasonable) but of the means utilized to protect it. The written regulations, formulated mostly with physical technology and proprietary software in mind, are ill-suited for achieving important security interests when these are bound up in freely available technology.

At the same time, the case offers important lessons about the leeway courts are willing to grant regulatory agencies struggling to adapt their regulations to new technologies. One such lesson is that ITAR's public domain exemption has some enforceable limits. In *Defense Distributed*, the court enforced these limits by appealing to the connection between the information offered and plainly military usage. Nevertheless, given the vague definition of technical data under ITAR, there is room to wonder how far the State Department and the courts would be willing to stretch the interpretation of the regulations, which currently seems to apply on a case-by-case basis. This leaves the door open to stringent interpretations that may, in theory if not in practice, apply to dual-use items. On the other hand, the ambiguity inherent in the regulations' current phrasing could also conceivably lend itself to much more permissive standards for publication and dissemination of information and software online.[101]

Though firearms present a clear military threat when compared with most software, the arguments made in *Defense Distributed*, and the federal court's response to them, are instructive for the question of software regulation more generally. The court's interpretation will likely be tested again as *Defense Distributed* and its tributary cases continue to make their way through the federal court system. In the meantime, the case has seen a few developments which exemplify contemporary software and data regulatory challenges.

In 2018, Defense Distributed and the Second Amendment Foundation accepted a settlement offer from the State Department which included a recognition that the CAD files were "approved for public release (i.e., unlimited distribution) by the cognizant U.S. Government

101. The DDTC has thus far only attempted to regulate technical data with a clear military application via ITAR, and there is no reason to believe that it will shift to anything broader any time soon. Nonetheless, this section highlights the possible ways regulators can utilize ITAR more broadly, as well as courts' willingness to accommodate expansive interpretations when a national security interest is at stake.

department or agency."[102] Notably, this ITAR exemption is separate from the public domain exemption and does not require publication.[103] The settlement is therefore not applicable to FOSS generally, since it requires prior review by a government agency. In order to allow for the publication of future CAD gun designs, it also includes a commitment on the part of the U.S. government to draft a regulatory rule excluding similar technology from the USML. Consequently, the BIS published a rule in 2020 which included a transfer of some firearms and related technology from the USML to the CCL.[104] The rule included an important alteration to the EAR's definition of "published," so that software used for the production of firearms would remain subject to the regulations despite its public availability.[105] Several states challenged both parts of the settlement, resulting in orders which have temporarily stayed their implementation.[106]

Within this convoluted train of events, a story emerges of a regulatory framework struggling to maintain a grasp on at least some parts of FOSS, however weakly. On the one hand, the transfer of categories from the USML to the CCL forms part of the deregulatory trend which marks the general attitude of export controls towards publicly available information, including software. On the other, the alteration of the language of the EAR's public availability exemption maintains

102. Settlement Agreement at 2, Def. Distributed v. U.S. Dep't of State, 121 F. Supp. 3d 680 (W.D. Tex. 2015); *see also* Cyrus Farivar, *3D-Printed Gun Lawsuit Ends After 3+ Years–in Gun Publisher's Favor*, ARSTECHNICA (Jul. 17, 2018), https://arstechnica.com/tech-policy/2018/07/3d-printed-gun-lawsuit-ends-after-3-years-in-gun-publishers-favor/.

103. *See* 22 C.F.R. § 125.4(b)(13) (2016).

104. *See id.*; Control of Firearms, Guns, Ammunition and Related Articles the President Determines No Longer Warrant Control Under the United States Munitions List (USML), 85 Fed. Reg. 4136 (Jan. 23, 2020).

105. 15 C.F.R. § 734.7(c) (2020). The full text of the amended subsection is as follows: "The following remains subject to the EAR: 'software' or 'technology' for the production of a firearm, or firearm frame or receiver, controlled under ECCN 0A501, that is made available by posting on the internet in an electronic format, such as AMF or G-code, and is ready for insertion into a computer numerically controlled machine tool, additive manufacturing equipment, or any other equipment that makes use of the 'software' or 'technology' to produce the firearm frame or receiver or complete firearm."

106. Washington v. U.S. Dep't of State, 420 F. Supp. 3d 1130, 1137–38 (W.D. Wash. 2019); Washington v. U.S. Dep't of State, 443 F. Supp. 3d 1245, 1262–63 (W.D. Wash. 2020). The BIS responded to the latter injunction by issuing Control of Firearms, Guns, Ammunition and Related Articles the President Determines No Longer Warrant Control Under the United States Munitions List (USML); Notifying the Public of the Bureau's Interim Measures With Respect to March 6, 2020 Court Order, 85 Fed. Reg. 18,438 (Mar. 6, 2020). It should be noted that mirrors of the gun CAD files are available on other websites, including GitHub, which do not seem to have been targeted for removal pursuant to ITAR thus far.

some semblance of a regulatory hook. It is unclear what protection this shift affords in practice. Clearly, however, regulators struggle to find legal mechanisms that would allow them to limit the spread of publicly available firearm designs, despite *Defense Distributed*'s nod to an evident national security interest.

From a different perspective, *Defense Distributed* can also be viewed as an attempt by the Defense Department to regulate data, rather than software. In this regard, the prolonged court battle resulting in the limitation on the distribution of such data stands in contrast with the relatively relaxed approach to FOSS regulation. The complementarity of the two types of regulation (over data and over software) is revealed by the strengthening of controls over software when controls over data are slackened. The DDTC's behavior, however, shows that its first regulatory interest is in data, and the regulation of software is secondary, resorted to only when the first has failed.

B. U.S. Export Restrictions on Encryption

The intertwined development of export controls and FOSS is marked by the response of each of these forces to the other and by the corresponding changes these responses bring about. Thus far, this Note has explored the accelerated growth in FOSS as well as the regulatory landscape which enabled and supported it. Section A also investigated how FOSS continually shapes the minutiae of export control regulations. Section B applies the same treatment to encryption, a special subset of regulated technology. Historically, export restrictions on FOSS-based encryption were tighter than on FOSS; their loosening is therefore particularly instructive for understanding how national security interests interact with technological evolution.

More generally, the regulation of encryption via export restrictions raises important questions about the role of the government in regulating the internet as a whole. Encryption is tightly bound up in technological solutions for online privacy and free speech. Thus, any policy limitation placed on encryption must carefully consider its impact on these two interests, along with potential national security concerns. Moreover, and perhaps more pertinently, open source encryption has become an important component of FOSS in recent years. For these reasons, the examination of encryption can also help to illuminate some of the contemporary tensions between regulation and innovation online.

Until the 1990s, practically all encryption software was classified as "defense articles" and thus subject to export controls under

ITAR.[107] In order to ease some of the regulatory burden and improve commerce, jurisdiction over "commercial encryption products" was transferred in 1996 from the State Department to the Commerce Department and subjected to the EAR thereafter, although ITAR continued to govern encryption products designed or modified specifically for military use. This regulatory regime was still comparatively stringent and made export and reexport of any encryption technology very difficult.[108]

Since then, relevant regulations have undergone numerous changes that liberalized the export process. The pressure levied by a coalition of tech industry and civil liberties groups, coupled with judicial rulings on the expressive aspects of software,[109] have had the effect of evolving export controls "from case-by-case licensing of individual encryption exports . . . to broad approvals for exports to certain preferred industry sectors, and finally to nearly free exportability of most products with after-the-fact reporting."[110] Much of this was done in a piecemeal fashion, with the result that contemporary controls are still quite complex and overlapping. For the sake of the present discussion, it suffices to examine current controls placed on open source encryption without delving too deeply into their history.[111]

ITAR classifies the types of encryption it regulates into very specific categories, covering items defined as "military or intelligence."[112] Therefore, most open source cryptographic software does

107. Ira S. Rubinstein & Michael D. Hintze, *Export Controls on Encryption Software*, *in* COPING WITH US EXPORT CONTROLS § 3(a) (E. Berlack & C. Hunt eds. 2000).

108. Corr, *supra* note 35, at 484–85.

109. *See supra* notes 34–35.

110. Rubinstein & Hintze, *supra* note 107, at § 5.

111. For a more in-depth overview, see generally Rubinstein & Hintze, *supra* note 107; LIEBMAN ET AL., *supra* note 38, at § 6.

112. Category XIII of 22 C.F.R. § 121.1 (2020):

> (1) Military or intelligence cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components, and software (including their cryptographic interfaces) capable of maintaining secrecy or confidentiality of information or information systems, including equipment or software for tracking, telemetry, and control (TT&C) encryption and decryption;
>
> (2) Military or intelligence cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components, and software (including their cryptographic interfaces) capable of generating spreading or hopping codes for spread spectrum systems or equipment;
>
> (3) Military or intelligence cryptanalytic systems, equipment, assemblies, modules, integrated circuits, components and software.

not qualify, since it is not usually designed specifically for military or intelligence purposes. This is not to say that all encryption software posted online is automatically exempt from ITAR regulation, but this is a much better defined category than ITAR's ambiguous definition of qualifying software. Additionally, the rationale underpinning the transfer of encryption from the jurisdiction of the DDTC to the BIS was to avoid the stringency of ITAR. Such a rationale would not be served if open source cryptography was still broadly subject to ITAR controls.

When situated within the EAR scheme, open source code and object code derived from open source codes[113] are exempt from regulation under the public availability exemption, with the caveat that their exporters must provide notification to the government if the cryptography is "non-standard." Non-standard cryptography includes proprietary and previously unpublished cryptographic implementations.[114] Before March 2021, exporters who made any open source cryptographic code publicly available had to notify the BIS and the ENC Encryption Request Coordinator at the National Security Agency, via e-mail, with one of the following: (1) the URL where the encryption source code has been published, or (2) a copy of the published encryption source code.[115] Newer regulations now allow for the

---

113. The relevant definitions under EAR can be found in 15 C.F.R. § 772.1 (2021):
> *Encryption items*. The phrase encryption items includes all encryption commodities, software, and technology that contain encryption features and are subject to the EAR. This does not include encryption items specifically designed, developed, configured, adapted or modified for military applications (including command, control and intelligence applications) which are controlled by the Department of State on the U.S. Munitions List.
>
> . . .
>
> *Encryption object code*. Computer programs containing an encryption source code that has been compiled into a form of code that can be directly executed by a computer to perform an encryption function.
>
> *Encryption software*. Computer programs that provide capability of encryption functions or confidentiality of information or information systems. Such software includes source code, object code, applications software, or system software.
>
> *Encryption source code*. A precise set of operating instructions to a computer that, when compiled, allows for the execution of an encryption function on a computer.

114. "Non-standard encryption" is "any implementation of 'cryptography' involving the incorporation or use of proprietary or unpublished cryptographic functionality, including encryption algorithms or protocols that have not been adopted or approved by a duly recognized international standards body (e.g., IEEE, IETF, ISO, ITU, ETSI, 3GPP, TIA, and GSMA) and have not otherwise been published." *Id.*

115. *See* Cindy Cohn & Andrew Crocker, *US Export Controls and "Published" Encryption Source Code Explained,* ELEC. FRONTIER FOUND. (Aug. 27, 2019), https://

publishing of cryptographic code with no notification if the encryption had previously been made publicly available.

The BIS explicated the current model in the context of changes made to the EAR in 2016.[116] Under this modern interpretation, there are no regulatory export prohibitions on posting encryption software online for free. Thus, open source encryption software is, by definition, not subject to EAR controls—although, unlike with FOSS in general, a notification requirement for novel cryptography continues to exist. Presumably, the rationale for notification stems from the intelligence community's need to keep abreast of new encryption capabilities which might limit their activity. It should be noted that proprietary software incorporating FOSS or open source encryption is still regulated by the EAR.[117]

The bottom line is that there is less ambiguity about the regulation of FOSS encryption than FOSS more generally. By and large, encryption published online is exempt from the regulatory schemes discussed thus far, or, if the encryption is novel, it is subject to a relatively loose reporting requirement.

---

www.eff.org/deeplinks/2019/08/us-export-controls-and-published-encryption-source-code-explained [https://perma.cc/H8ZM-43Q8]; 15 C.F.R. § 742.15 (2021) (omitting these requirements).

116. 2016 Revisions, *supra* note 61.

117. Cohn & Crocker, *supra* note 115.

TABLE II: SUMMARY OF REGULATIONS

Regulation	Administering Body	Regulation Affecting FOSS	Regulation Affecting FOSS-based Encryption
Export Administration Regulations (EAR)	Bureau of Industry & Security (BIS) within the Commerce Department	- Regulates dual use software - Public availability exemption applies	- Regulates most encryption software - Public availability exemption applies (subject to notification for non-standard encryption)
International Traffic in Arms Regulations (ITAR)	Directorate of Defense Trade Controls (DDTC) within the State Department	- Regulates military software - Ambiguity as to whether public availability exemption applies - Does not affect most FOSS	- Regulates military or intelligence encryption software (narrowly construed) - Requires a license
Trade Sanctions	Office of Foreign Assets Control (OFAC) within the Treasury Department	- Regulates software exported to sanctioned countries - Appears to include implicit exemption for FOSS in the public domain - Affects OpenSaaS	- Regulates software exported to sanctioned countries - Appears to include implicit exemption for FOSS in the public domain - Affects OpenSaaS

C. Regulatory Interventions

The export restrictions described above, although often criticized for being technologically anachronistic,[118] are constantly evolving.

118. This has been a frequent running commentary from practitioners. *See, e.g.*, Reid Whitten & Lisa Mays, *A Wave of Export Regulation to Hit US Technologies*, SHEP-

Strategically broad, especially in the areas that are closest to the core of national security interests, regulations are designed to balance between the government's need to control harmful materials and information and civil society's need to advance knowledge and develop new technologies. At the same time, they contain exemptions that place publicly available software mostly outside of their ambit. Branching out from the particulars of each regulatory regime detailed in sections A and B, this section offers a summary overview and some examples of the export control dialectic, with particular emphasis placed on areas where regulatory interventions do affect the development of FOSS.

From a historical perspective, the various administrative agencies in charge of enforcing the regulations have, sometimes begrudgingly, loosened their regulation on FOSS gradually. The first major step in this direction was a series of court cases concerning encryption, which forced the State Department to allow some publication of encryption in public fora.[119] EAR controls have also significantly loosened, most recently in 2016, with the broadening of the definition of "public domain" and the explicit inclusion of the internet as a publishing medium.[120]

As seen in section B, EAR controls explicitly exempt software which is publicly available—that is, software that is published or will be published. Pursuant to the recent clarification by BIS regarding encryption, this exception fully applies to FOSS, which by its nature is freely available to anyone wishing to access it. The EAR therefore present no hindrance to the publication of FOSS online, although there is a slight caveat mandating that "non-standard" cryptographic code must be reported to the BIS and the NSA.

OFAC similarly places no restrictions on the export of FOSS due to a similar publication exemption. However, OFAC sanctions apparently limit fee-based SaaS, and presumably also OpenSaaS, which is FOSS-based software as a service (often offered on a subscription basis). As an example of this dynamic in practice, consider WordPress,

---

PARD MULLIN: GLOBAL TRADE L. BLOG (Apr. 10, 2019), https://www.globaltradelawblog.com/2019/04/10/export-regulation-us-technologies/ [https://perma.cc/ECS7-UTJM]; *Regulation and Legislation Lag Behind Constantly Evolving Technology*, BLOOMBERG L. (Sept. 27, 2019), https://pro.bloomberglaw.com/regulation-and-legislation-lag-behind-technology/ [https://perma.cc/X57T-VRMA].

119. *See* Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426 (N.D. Cal. 1996), *aff'd sub nom*. Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132 (9th Cir. 1999), *withdrawn and reh'g granted*, 192 F.3d 1308 (1999); Junger v. Daley, 209 F.3d 481 (6th Cir. 2000).

120. 2016 Revisions, *supra* note 61.

whose source code is licensed under a free software license (GNU GPL), and may thus be used freely by anyone who abides by the license's terms. Automattic, the web development company founded by one of Wordpress's software developers, additionally offers consumers the option of using a ready-made blogging platform that implements the WordPress source code. The platform takes the form of a turnkey product hosted on WordPress.com and supported by Automattic. This product comes in a range of different "plans," only one of which is free and offers limited features.

OFAC controls would have no regulatory hook for limiting the publication of the WordPress FOSS. Instead, its regulations would allow it to limit the services Automattic offers, particularly the paid versions. OFAC's control over the latter is especially broad when the services are offered for use in embargoed countries. This could mean, for example, that OFAC would theoretically be able to limit Automattic's ability to offer a ready-made paid-for platform in North Korea.

Another example of the distinction between services and software can be found in GitHub's 2019 decision to bar access to private repositories and paid services on GitHub.com for individuals and organizations located in sanctioned regions (Crimea, Cuba, Iran, North Korea and Syria), citing OFAC restrictions.[121] GitHub is a Microsoft-owned company providing cloud hosting for software development, which considers itself a "hub" for FOSS projects. GitHub.com's source code is proprietary and some of the services it offers, such as phone or web-based support, are fee-based. Other services, such as free private repositories for individual users, are not. When GitHub.com announced its decision to limit access to embargoed countries, it made a distinction between access to public software repositories, and additional services and tools provided and developed by GitHub. Organizations and individuals from embargoed countries can still access the public repositories and thus have access to the

121. *GitHub and Trade Controls,* GITHUB, https://help.github.com/en/github/site-policy/github-and-trade-controls [https://perma.cc/CFY6-TYTP] (last visited May 24, 2020) ; Tyler Fuller, *Global Software Collaboration in the Face of Sanctions*, GITHUB BLOG (Sept. 12, 2019), https://github.blog/2019-09-12-global-software-collaboration-in-the-face-of-sanctions/ [https://perma.cc/3P87-PQQ2]. In early 2021, GitHub sought and obtained a special license from OFAC to provide services to individuals located in Iran. *See* Nat Friedman, *Advancing Developer Freedom: GitHub is Fully Available in Iran*, GITHUB BLOG (Jan. 5, 2021), https://github.blog/2021-01-05-advancing-developer-freedom-github-is-fully-available-in-iran/ [https://perma.cc/TK3J-ARS7].

software itself, but GitHub is barred from extending services to them.[122]

In an attempt to avoid liability for OFAC sanction violations, some distributors of FOSS add disclaimers to downloads of their software,[123] or adopt a "don't ask, don't tell" policy regarding the nationality of contributors.[124] Thus, they are able to argue that they do not have knowledge of individuals from embargoed countries downloading or contributing to FOSS.[125] This obfuscation is testament to the ambiguous and confusing nature of a sanctions regime which does not thoroughly clarify its stance on FOSS. It is patently evident that such disclaimers do not materially implement any sanctions, since nothing is barring a person located in Crimea, for example, from accessing the software and downloading it while ignoring the disclaimer (which is generally buried in the website's policy and terms anyway). At the same time, some argue that undertaking more aggressive blocking mechanisms (such as geoblocking) would undermine the collaborative aspect of FOSS and risk further alienating oppressed communities in embargoed countries.[126]

Another challenge to the free publication of FOSS comes from ITAR. Due to the problematic and expansive regulatory structure imposed in the name of national security, many pieces of otherwise in-

122. It is worth noting that this is a comparatively expansive solution to the problem. Google used to have a similar hosting site named Google Code, but prohibited access by "users residing in countries on the United States Office of Foreign Assets Control sanction list, including Cuba, Iran, North Korea, Sudan and Syria". *See Additional Terms: Google Project Hosting*, GOOGLE CODE, https://code.google.com/projecthosting/terms.html (last visited Jan. 13, 2020).

123. *See, e.g.*, *Fedora Export Compliance/Customs Information,* FEDORA WIKI https://fedoraproject.org/wiki/Legal:Export (last updated Sept. 6, 2017) [hereinafter *Fedora Export Terms*].

124. Michael Larabel, *Fedora to Have a "Don't Ask, Don't Tell" for Contributors*, PHORONIX (Mar. 5, 2014), https://www.phoronix.com/scan.php?page=News_item&px=MTYyMjg.

125. The Free Software Foundation views this as a legal risk reduction measure rather than a requirement. *Frequently Asked Questions About the GNU Licenses: Export Warranties*, GNU OPERATING SYS., https://www.gnu.org/licenses/gpl-faq.en.html#ExportWarranties (last updated Jan. 1, 2020).

126. See Baker, *supra* note 72, at 552–63 for an analogous argument regarding internet services. Baker provides examples of the way sanctions incentivize companies to discontinue services to citizens of embargoed countries, even when service provision is ostensibly legal, and argues that implicated "internet and communications technologies" are effective tools for the promotion of human rights. Thus, sanctions which aggressively limit their dissemination undermine the work of dissidents and human rights advocates in embargoed countries. In a similar vein, lightening sanctions may lead to services and FOSS to be used in the service of authoritarian governments, but these have more resources at their disposal and will much more easily be able to bypass blocking measures (including geoblocking).

nocuous software could be made subject to ITAR. However, there is little reason at present to believe that the government would bring suit against developers or distributors of FOSS that has no immediate military applications. Furthermore, there are some limits that can be extrapolated from *Defense Distributed*, where the court stressed several times that national security concerns do not always win the day.

It is also clear from prominent industry players that ITAR controls are not considered a serious impediment to development in most cases. Consider Linux, for example, which views the EAR as effectively exempting all Linux Foundation FOSS projects, including those that include encryption (with the notification caveat in place).[127] Other FOSS projects and companies have made statements to a similar effect.[128] These do not really contemplate the impact of ITAR regulations, and some make no mention of OFAC sanctions at all. Nevertheless, it is evident that there are still many grey areas in the legal regulatory landscape, particularly where OFAC is concerned. These deserve more explicit recognition and would benefit from direct dialogue with the burgeoning FOSS community, particularly given its growing dominance in software ventures.

The regulatory interventions described here impact mostly the periphery of FOSS development. This is the result of the mismatch of FOSS, with its particular attributes, and export controls, with their particular tools. The challenge of regulating FOSS effectively, so that it can continue to drive innovation while curbing more dangerous technological developments, continues to loom large. This challenge echoes the larger problem regulatory agencies face when attempting to corral publicly available data. This similarity is part of the reason regulators have shifted their attention to regulating data, rather than software. This displacement of regulatory effort, explored below in Part IV, sheds light on the future of regulatory intervention on the internet.

127. *Linux Foundation Statement on Huawei Entity List Ruling,* LINUX FOUND. (May 23, 2019), https://www.linuxfoundation.org/blog/2019/05/linux-foundation-statement-on-huawei-entity-list-ruling.

128. Roman Shaposhnik, *Statement by the Apache Software Foundation Regarding US Federal Register Notice of Non-US Affiliates Added to Entity List Ruling,* APACHE SOFTWARE FOUND. BLOG (May 22, 2019), https://blogs.apache.org/foundation/entry/statement-by-the-apache-software; *Fedora Export Terms*, *supra* note 123.

IV.
PATHWAYS TO REGULATING FOSS

The bottom line of the foregoing discussion is that FOSS *qua* FOSS, aside from a few notable exceptions, is currently not regulated by the export control scheme. This Part examines the implications of this state of affairs. The first section discusses whether the non-regulation of FOSS poses national security risks. The second section looks at the ways the U.S. government has maintained a handle on the outputs of FOSS, while not controlling the software itself. This last section then argues that governments do still possess tools for "quarantining" certain aspects of FOSS. The relative weakness of this approach can help to explain, at least in part, the displacement of software regulation onto data.

A. Responding to Risk

Attempts by U.S. administrators to regulate software are often met with significant industry pushback. An update to the EAR which includes restrictions on "artificial intelligence" is but the most recent example. Even though policymakers acknowledge that the core of much of the software powering artificial intelligence (AI) is in the public domain, there have been reports that the BIS will move to restrict certain implementations of it.[129] Here, as elsewhere in the export restriction debate, industry giants such as Google and Microsoft are urging the U.S. government to tread lightly so as not to inhibit technological advances and thus limit their competitive edge.[130]

---

129. Metz, *supra* note 33.

130. Neil Martin & Tim Willis, *Google, The Wassenaar Arrangement, and Vulnerability Research*, GOOGLE: SEC. BLOG (Jul. 20, 2015), https://security.googleblog.com/2015/07/google-wassenaar-arrangement-and.html [https://perma.cc/4YKL-K6XW] (opposing a 2015 amendment to the EAR on the grounds that it "would negatively affect vulnerability research"); Alan Cohn, *Export Controls: The Next Frontier in Cybersecurity?*, MICROSOFT: EU POL'Y BLOG (Apr. 13, 2017), https://blogs.microsoft.com/eupolicy/2017/04/13/export-controls-the-next-frontier-in-cybersecurity (opposing a change to the Wassenaar Agreement and in EU legislation that would regulate "cyber-surveillance technology"); Microsoft, Comment Letter on Advance Notice of Proposed Rulemaking Regarding Review of Controls for Certain Emerging Technologies (Jan. 10, 2019), https://www.regulations.gov/document?D=BIS-2018-0024-0175 (arguing that a "traditional list-based control regime could thwart U.S. interests. The technologies are in worldwide development and there is robust research and deployment of them internationally for commercial and consumer uses"); Facebook, Comment Letter on Advance Notice of Proposed Rulemaking Regarding Review of Controls for Certain Emerging Technologies (Jan. 10, 2019), https://www.regulations.gov/document?D=BIS-2018-0024-0212 (arguing that "[e]xport controls risk slowing innovation, and the hiring and retention of top researchers in the United States); Google, Comment on Advance Notice of Proposed

Increasingly, traditional methods of export control are coming up against a wall: how does a government restrict access to technologies that might threaten its national security? In order to determine the answer to this question, technologies must be categorized into those that threaten national security and those that do not. Because export regulations have, by and large, given up on the idea of regulating FOSS, they have also conceptually excluded the idea that publicly available technologies pose a threat. But is this view correct?

Consider, for example, FOSS-based drone enterprises, such as the Linux-affiliated Dronecode Foundation, which supports projects that provide, among other things, flight control and communication protocol software.[131] Certain military and civilian drones are regulated under ITAR and EAR.[132] However, due to the public availability exemption, Dronecode-like software is generally not regulated. This creates a strange state of affairs given the security risk it poses,[133] due to its adaptability for reconnaissance, for example.[134] As with other FOSS, if the same software was offered in a proprietary manner for civilian purposes, it would be regulated by the EAR.[135] Moreover, the application of ITAR to this software would be even more difficult than in *Defense Distributed* because there is considerable ambiguity about its use. The limitations imposed in *Defense Distributed* begin to break down the further the software goes from clear military applications.

Even if such a commercial product would likely receive a license under the EAR, the licensing scheme as a whole allows administrative

---

Rulemaking Regarding Review of Controls for Certain Emerging Technologies (Jan. 10, 2019), https://www.regulations.gov/document?D=BIS-2018-0024-0160 (arguing that "[u]nilateral controls of broad technology areas like AI would make it more difficult for companies like Google to compete, impede our ability to innovate, cause delays in product launches, and potentially block access to currently available products").

131. DRONECODE FOUNDATION, https://www.dronecode.org/ (last visited Sep. 13, 2020).

132. For an overview of the different ways EAR and ITAR regulate UAVs, see STIMSON CTR., UAV EXPORT CONTROLS AND REGULATORY CHALLENGES: WORKING GROUP REPORT 10–13 (2015), https://www.stimson.org/wp-content/files/file-attachments/ECRC%20Working%20Group%20Report.pdf.

133. The U.S. Government Accountability Office identified the development and deployment of unmanned vehicles as emerging threats facing the United States. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-204SP, LONG-RANGE EMERGING THREATS FACING THE UNITED STATES AS IDENTIFIED BY FEDERAL AGENCIES 8 (2018), https://www.gao.gov/assets/700/695981.pdf.

134. This threat is heightened given the proliferation of open hardware specifications and products which are, at best, minimally regulated. *See, e.g.*, PIXHAWK, https://pixhawk.org (last visited Sept. 13, 2020) (an open hardware project which provides hardware designs for drones, which are compatible with drone FOSS).

135. 15 C.F.R. § 774 Supp. 1, at ECCN 9D001.

agencies to maintain some control and dialogue with the relevant industry in order for the agency to keep abreast of new risks. Because the drone software is automatically in the public domain, it is theoretically unmonitored (although a regulator could, of course, monitor public repositories and maintain some knowledge of developments).

As this example illustrates, the exclusion of FOSS from the purview of most export controls, coupled with its rising importance in software development, has opened up a national security blindspot. This oversight is compounded by the problem of malicious code. "Legitimate" FOSS is vulnerable to the insertion of malware "back doors" —allowing hackers surreptitious access to computers utilizing the software—and of disruptive code such as ransomware. Additionally, some malware which is designed and disseminated in bad faith is also FOSS-based. Regulators, however, have a limited ability to directly engage with the proliferation of FOSS-based malware, at least in part due to the ineffectiveness of export controls and the exclusion of FOSS as a relevant target for regulatory oversight.[136] As the next section details, there are different approaches to dealing with these problems, some of which are adopted by U.S. regulators and some which are only potential alternatives to current regulatory measures.

B. Alternative Regulatory Measures and Displacement

One possible check on dangerous or malicious applications of FOSS comes from the FOSS community itself. Many development websites have terms that limit the kind of FOSS they are willing to host, and allow a "founding" user, or a central user or users, to maintain controls of official changes in the FOSS code of a specific project. Assuming these central agents are acting in good faith, this can curb the spread of malicious code. Additionally, some identify the structure of FOSS itself as strengthening the safety of the code; because it is freely available, more eyes can examine it critically and debug it.[137]

Unfortunately, the promise of these two avenues may be exaggerated. A recent study has shown that there are in fact fewer people than generally thought who control a large number of important projects, and that malicious code, or merely bad code, often gets overlooked for

136. For a report on the (ineffective) use of export controls in an attempt to curb the spread of malware, see TREY HERR, COUNTERING THE PROLIFERATION OF MALWARE: TARGETING THE VULNERABILITY LIFE CYCLE (Jun. 2017), https://www.belfercenter.org/sites/default/files/files/publication/CounteringProliferationofMalware.pdf

137. Raymond, *supra* note 8, at 30–36.

long stretches of time.[138] As more companies pay their developers to actively maintain and debug FOSS,[139] this problem may diminish, but at present regulators cannot rely on these as protections against national security threats.

Lest this Note be read as a call for strict regulation of FOSS, it is important to note that the current state of affairs affords FOSS developers, and many American corporations among them, the flexibility to collaboratively develop complex products and services that in the long run end up serving the interests of the American economy and security.[140] In many ways, this is a situation that a country should seek to maintain and safeguard. However, there is also room to consider a better balance between competing interests.[141] Such a balance need not necessarily be drawn within the framework of export controls, given its problems. Indeed, it may well be that a new or different regulatory framework is needed in response to this challenge of the digital age.

On a practical level, the implications here are twofold: first, that the defense and national security communities should (and probably already do) take note of developing FOSS that might threaten vital national security interests. This can be accomplished through robust dialogue with the industry or through a mandatory reporting scheme, such as the one employed for encryption. The recent attempts to up-

138. Markus Zimmermann, Cristian-Alexandru Staicu, Cam Tenny & Michael Pradel, *Small World with High Risks: A Study of Security Threats in the npm Ecosystem*, PROC. OF THE 28TH USENIX SEC. SYMP. 995 (2019), https://www.usenix.org/conference/usenixsecurity19/presentation/Zimmerman.

139. *2020 Open Source Program Survey Results*, TODO GROUP, https://github.com/todogroup/survey/tree/master/2020 (last visited Dec. 1, 2020) (survey among various technology companies showing high engagement among companies with open source initiatives, including contributing and sponsoring such projects).

140. For a perspective on this see Google, *supra* note 130; Robert D. Williams, *In the Balance: The Future of America's National Security and Innovation Ecosystem*, LAWFARE (Nov. 30, 2018 3:01 PM), https://www.lawfareblog.com/balance-future-americas-national-security-and-innovation-ecosystem; Robert D. Williams, *The Innovation-Security Conundrum of U.S.-China Relations*, LAWFARE (Jul. 24, 2018 8:21 AM), https://www.lawfareblog.com/innovation-security-conundrum-us-china-relations.

141. The focus of this Note is on the traditional concerns of export controls: national security vs. economic expansion, and it attempts to show the ways in which even this central balance is not particularly well calibrated. However, other interests are obviously also important and underrepresented in the balancing process. In particular, the way in which the U.S. government has leveraged export controls for surveillance purposes implicates privacy concerns of U.S. citizens and foreigners alike, and deserves more thorough consideration. For a perspective on this, see Cohen, *supra* note 4, at 111–12; Avidan Y. Cover, *Corporate Avatars and the Erosion of the Populist Fourth Amendment*, 100 IOWA L. REV. 1441, 1476 (2015).

date the EAR in order to account for developments in AI can be seen as the beginning of a dialogue, though it remains to be seen what the new rules will actually include, and what impact, if any, they will have on FOSS.

Second, as more private and governmental actors harness the power of FOSS, the more vulnerable they become to bugs in such software. Many vulnerabilities can ultimately be attributed to the shockingly low number of people functionally maintaining the infrastructure of FOSS (as was exemplified by the Heartbleed cybersecurity vulnerability found in OpenSSL, a widely used open source cryptographic software).[142] Therefore, the government itself has an interest in helping to maintain this type of software, especially when it has chosen not to regulate its export (the very thing that makes it so open to the scrutiny of bad-faith actors looking to exploit its vulnerabilities).[143]

Additionally, the U.S. government has shown that it possesses two other powerful tools at its disposal when it comes to the regulation of FOSS. First, as seen in *Defense Distributed*, in cases of blatant military application, ITAR still very much regulates, even if the material is placed in the public domain. This seems to be a "hard limit" that does somewhat fence FOSS in. It is a check against certain kinds of bad-faith applications that carry with them explicit military risk.

The second regulatory tool may be found in OFAC sanctions' regulation of services, and thus of SaaS.[144] This is an important check on the monetization of FOSS, which presumably serves to curb some of its more mercenary applications, at least insofar as these are developed by American companies. It is worth noting, however, that there is nothing in the software itself to stop companies outside the United States from developing their own services based around the same FOSS. In certain situations, this may be impeded by American interventions that block access to FOSS repositories, like in the GitHub

142. Marco Carvalho, Jared DeMott, Richard Ford & David A. Wheeler, *Heartbleed 101*, 12 IEEE SEC. & PRIV. 63 (2014); Seth Rosenblatt, *Tech Titans Join Forces to Stop the Next Heartbleed*, CNET (Apr. 24, 2014 5:00 AM), https://www.cnet.com/news/tech-titans-join-forces-to-stop-the-next-heartbleed/.

143. There are some nascent examples of government contributions to FOSS. *See, e.g.*, *Open Source Policy*, 18F, https://18f.gsa.gov/open-source-policy/ (last visited Jan. 13, 2020) (describing the open source policy of the digital service delivery team within General Service Administration, which develops code (including FOSS) for other governmental agencies); Tod Newcombe, *Four Myths About Open Source in Government*, GOV'T TECH. (Dec. 19, 2018), https://www.govtech.com/opinion/Four-Myths-About-Open-Source-in-Government-Contributed.html.

144. *See supra* footnotes 122–127 and accompanying text.

model, but other times the development of such services may prove entirely doable.

Beyond the regulatory export restrictions already employed by the U.S., there are several other avenues that allow for the roundabout regulation of FOSS. Chief among these is the displacement of software regulation with data regulation, meaning the shifting of the regulatory subject from executable code to aggregated pieces of information.[145]

The regulatory terrain has gradually transformed towards a focus on data, in part due to the difficulties described above of wrangling software into manageable regulation, and in part due to the shift towards data-reliant software development which is sometimes tied to the rise of machine learning and "big data."[146] In this new landscape, data becomes powerful currency, and the access to it can be redefined as a national security risk. An instance of this conversion is explored below, along with some other regulatory mechanisms which function to constrain FOSS proliferation, albeit indirectly.

The first mechanism is exemplified by Executive Order 13873, titled "Securing the Information and Communications Technology and Services Supply Chain," which was signed by President Trump on May 15, 2019. The Order declared a national emergency with respect to "the unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries."[147] Therefore, the Order restricts inbound "transactions" (very broadly defined to include *inter alia* "use" and "transfer" of software, among other things) that pose "an unacceptable risk" to national security, and that are conducted with "foreign adversaries," to be designated by the

145. Very broadly, software means instructions which direct a computer to perform certain tasks, while data means content or information that can be processed or used in some way. In this sense, data can be processed by software.

146. As Mireille Hildebrandt explains, "the availability of very large data resources seems to reduce the need for highly sophisticated algorithms; at some point the sheer quantity of data augments the performance of the algorithms such that the choice of the algorithm becomes less relevant. This would imply that gathering large amounts of data is far more important than developing highly sophisticated algorithms and it seems to be that precisely this implication has led to a nearly religious reverence for what has been coined Big Data." (MIREILLE HILDEBRANDT, SMART TECHNOLOGIES AND THE END(S) OF LAW: NOVEL ENTANGLEMENTS OF LAW AND TECHNOLOGY 30 (2015), citing (in the first half of the quote) STUART RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH 28 (3rd ed. 2009)).

147. Securing the Information and Communications Technology and Services Supply Chain, Exec. Order No. 13873, 84 Fed. Reg. 22689 (May 17, 2019).

Commerce Department in consultation with other agencies.[148] These adversaries are defined as "any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons."[149]

Once the Commerce Department classifies these terms, the Executive Order will effectively function as an *import* restriction. Crucially, the language of the Order does not contain reference to a public availability exemption. Due to the nature of FOSS as an international collaborative effort, it could easily be classified as an import under the terms of the Order, as easily as it could be classified as an export under the EAR. This would be especially true given the fact that FOSS projects can sometimes be identified with particular companies or nations.[150]

The BIS has thus far only used the Order as a basis for listing the Chinese company Huawei on its Entity List.[151] The Order has therefore not had any impact on FOSS. However, its expansive language leaves the door open for future attempted restrictions. One potential argument against such a move could be that the exemption that applies to the EAR should also apply here where the very same action and software are concerned. The Order and the EAR are two different regulatory instruments, but the rationales underlying the EAR exemption, and in particular the issue of free speech, could possibly also apply to the Order.

Another method of regulation that could be implemented technologically is the enforcement of access restrictions to publicly available information. In much the same way as OFAC sanctions have "nudged" companies into posting disclaimers that attempt to prohibit people from sanctioned countries from making use of publicly available data, more advanced technological restrictions could be implemented to actively bar them. This may be done through more widespread geoblocking (for example, if GitHub decided to restrict access to all its

148. *Id*.

149. *Id*.

150. *See, e.g.*, Bryant Son, *The State of Open Source in South Korea*, OPENSOURCE (May 7, 2019), https://opensource.com/article/19/5/projects-south-korea.

151. The BIS listed Huawei on its Entity List because they had "a reasonable basis to conclude that Huawei is engaged in. . . alleged violations of the International Emergency Economic Powers Act (IEEPA), conspiracy to violate IEEPA by providing prohibited financial services to Iran, and obstruction of justice in connection with the investigation of those alleged violations of U.S. sanctions." *Huawei Entity List Frequently Asked Questions (FAQs)*, BUREAU OF INDUS. AND SEC. (Dec. 3, 2020), https://www.bis.doc.gov/index.php/documents/pdfs/2447-huawei-entity-listing-faqs/file.

repositories, both public and private, for users in certain locations, it could do so). Although this avenue is not currently pursued by OFAC, the wording of the relevant sanctions is relatively vague and could support the imposition of such restrictions in the future, although they would likely be challenged in court on the basis of freedom of speech. From a development standpoint, this would also lead to increased fragmentation within the FOSS community and could undermine important aspects of the enterprise. Effective enforcement would be particularly challenging.

Finally, an avenue which the U.S. seems to be pursuing more aggressively, especially in relation to China, is data regulation through the regulation of foreign investments. In particular, the Committee on Foreign Investment in the United States (CFIUS) reviews the national security implications of foreign investments in U.S.-based companies, and has in recent years increasingly focused on transactions that may result in foreign investors obtaining personal information of U.S. citizens. It is beyond the scope of this Note to examine the full statutory scheme undergirding the activity of the Committee, but a cursory overview of the Grindr sale will serve well as an example of the type of regulatory displacement discussed.

Beijing Kunlun Technology Company was ordered by CFIUS in March 2019 to sell its majority stake in Grindr, a popular American dating app catering to the LGBTQ community. Although the Committee did not comment on the matter publicly, it is widely believed that the issue at the heart of the order was the possibility that personally identifying information such as sexual orientation, HIV status, etc. would fall into the hands of a Chinese company and make its way through it to the Chinese government.[152] The fear is that this type of material may serve as fodder for blackmail attempts against Americans for Chinese governmental interests.

CFIUS's mandate in this case came from the 2018 Foreign Investment Risk Modernization Act (FIRRMA), which codified the Committee's practice of closely examining investments in American businesses that hold personally identifying information of Americans. In particular, the Act stipulates that active foreign investments in U.S. businesses that "[maintain] or [collect] sensitive personal data of United States citizens that may be exploited in a manner that threatens national security" constitute a covered transaction, potentially subject

152. David E. Singer, *Grindr Is Owned by a Chinese Firm, and the U.S. Is Trying to Force It to Sell,* N.Y. TIMES (Mar. 28, 2019), https://www.nytimes.com/2019/03/28/us/politics/grindr-china-national-security.html.

to review.[153] Although the Grindr example deals with proprietary software, it is not inconceivable that similar situations could arise regarding start-ups that utilize FOSS. The way the CFIUS has framed the issue, the problem is not with the software powering the app, but with data collection.[154]

This push towards the regulation of data rather than software is emblematic of the shift in regulatory thinking of American administrative agencies faced with rapid evolution in the technology sector. While the fight over the availability of FOSS may have been mostly won, an important question remains of how the regulation of data will influence the regulation of software, particularly FOSS. Certainly in the Grindr case, as in the OFAC restrictions on services, data restrictions provide an important hindrance to the monetization of software, and thus of FOSS as well. This may have more severe implications for applications of FOSS that are intertwined with databases or datasets comprised of personally identifiable information. At the same time, regulating data is not the same as regulating code, and some vulnerabilities in FOSS, such as issues with malicious or buggy code, may persist.

As regulators continue to grapple with how to best balance national security and economic expansion, the subject of regulation may change, but the core issues remain the same. At base, the proliferation of software generally and FOSS specifically challenges entrenched regulatory structures because of how publicly it is developed and circulated. The attempt to corral software-driven data mining practices is but the latest attempt to isolate troublesome technologies into more manageable boxes. The more these boxes expand to accommodate

153. Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115–232, §1703(a)(4)(B)(iii)(III), 132 Stat. 1636, 2178. For a discussion of the ambiguities baked into some of the most salient terms enacted into the statute, see J. Russell Blakey, Note, *The Foreign Investment Risk Review Modernization Act: The Double-Edged Sword of U.S. Foreign Investment Regulations*, 53 LOY. L.A. L. REV. 981 (2020).

154. A similar dynamic appears to have played out in the CFIUS's review of ByteDance's acquisition of the predecessor to TikTok. Executive Order Number 13942 specifically mentions the fact that "TikTok automatically captures vast swaths of information from its users, including internet and other network activity information such as location data and browsing and search histories. This data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information—potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage." Addressing the Threat Posed by TikTok, and Taking Additional Steps to Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain, Exec. Order No. 13942, 85 Fed. Reg. 48637 (Aug. 6, 2020).

previously publicly available material, the more difficult they will be to regulate using current export control tools.

Conclusion

Export controls are an important tool governments can use to protect the security interests of their country and citizenry. They allow for the sequestering of certain items that have the potential to cause harm if they fall into the wrong hands. These limitations come at a cost, and thus must be balanced against other important national interests, namely economic expansion and the protection of liberties. This already complex interest equation becomes even more complicated when the export at hand is by nature freely available and collaboratively produced, as most FOSS is.

In the preceding pages, this Note argued that the U.S. government has responded to the challenges of modern software by attempting to force an ill-fitting framework to accommodate FOSS. While black-letter law is often ambiguous or intentionally broad, in practice most FOSS development online is unencumbered by government regulation. At the same time, as awareness of potential harms resulting from emerging FOSS-based technologies grows, regulatory bodies have attempted to set some limits on the proliferation of FOSS, either through the direct imposition of export controls or through other, more circuitous, means, such as the regulation of data. Developers and companies reliant on FOSS-fostered technology have met these restrictions with varying degrees of resistance.

The difficulty of regulating software in general, and FOSS in particular, is not unique to export controls. Other fields of law, including copyright and patent law, have also met with considerable challenges in this regard. In intellectual property, as in export controls, this has led in some cases to a shift towards the regulation of data. The full implications of this displacement are ripe for further study. This Note only goes as far as developing an overview of one of its main causes, namely the challenges of regulating increasingly public software. The equilibrium struck by U.S. export control administrators is indicative of the kind of compromises and decisions necessary in attempting such regulation within the current framework. At the same time, the interplay between FOSS development and its regulators serves as a case study of technology routing around regulatory barriers. In an age of increasingly creative thinking about global and administrative internet governance, it may be time to rethink the frameworks that do the work of balancing national security against other interests.