2016

Regulating Software When Everything Has Software

Paul Ohm
Georgetown University Law Center

Blake Reid
University of Colorado Law School

Citation Information

Paul Ohm and Blake Reid, *Regulating Software When Everything Has Software*, 84 GEO. WASH. L. REV. 1672 (2016), *available at* https://scholar.law.colorado.edu/faculty-articles/19.

Regulating Software When Everything Has Software

Paul Ohm and Blake Reid†*

Abstract

This Article identifies a profound, ongoing shift in the modern administrative state: from the regulation of things to the regulation of code. This shift has and will continue to place previously isolated agencies in an increasing state of overlap, raising the likelihood of inconsistent regulations and putting seemingly disparate policy goals, like privacy, safety, environmental protection, and copyright enforcement, in tension. This Article explores this problem through a series of case studies and articulates a taxonomy of code regulations to help place hardware-turned-code rules in context. The Article considers the likely turf wars, regulatory thickets, and related dynamics that are likely to arise, and closes by considering the benefits of creating a new agency with some degree of centralized authority over software regulation issues.

Table of Contents

---

* Professor of Law, Georgetown University Law Center.

† Assistant Clinical Professor of Law, University of Colorado Law School. The Authors would like to thank the editors of *The George Washington Law Review* and the participants in the *Law Review*'s 2015 Symposium. Thanks also to participants at the Internet Law Scholars Conference. Special thanks to Ed Felten, Roger Ford, Josh Goldfoot, James Grimmelmann, Margot Kaminski, Orin Kerr, Michael Madison, and Phil Weiser.

December 2016 Vol. 84 No. 6

Introduction

2015 may someday be viewed as a major inflection point in the regulation of software in the United States. In that year, agencies that traditionally had very little to say about code and coders suddenly became aggressive regulators of code, from the Environmental Protection Agency ("EPA") to the Food and Drug Administration ("FDA") to the Federal Aviation Administration ("FAA").[1] From the Federal Communications Commission ("FCC"), we witnessed an agency with a long history of regulating the telecommunications infrastructure claw its way up the Open Systems Interconnection ("OSI") layer stack, focusing more than it had before on what happens at the Operating System and app layers and doing so in the way it regulated information privacy and wireless interference.[2] Legacy code-regulating agencies from the Department of Justice ("DOJ") to the Federal Trade Commission ("FTC") to the Copyright Office stepped up their activity in this space.[3]

This is not simply a story of agency mission creep and turf warfare, although that is part of the tale. This is, instead, the inevitable result of embedding software in everything. Physical functionality has been supplemented and replaced by code, thus digitizing the operation of everything from cars to thermostats to medical research.[4] Agencies and regulators had to respond, whether or not they wanted to. Some have embraced the job eagerly while others have been dragged into grappling with the digital age. For both groups, 2015 seemed to be the year that many realized that to regulate commerce, public

1 For case studies, see *infra* Section I.C.

2 *See infra* Section I.A.

3 *See infra* Part I.

4 *See infra* Part I.

safety, consumer protection, or any number of other areas is also to regulate code.[5]

In this Article, we begin to examine the implications of this shift. Our examination puts the coder (and many species thereof—the tinkerer,[6] the maker, the software engineer) at the center. The first task is to document the spread of code regulation, so we start with two notable case studies from 2015, with one telling the story of the FCC's attempts to regulate software-defined radios and the other detailing the year the Digital Millennium Copyright Act ("DMCA")[7] triennial review finally exploded well-beyond its original framing.[8] Synthesizing these examples, we create a taxonomy of code regulation, one we think can be used as a framework for organizing and analyzing discussions over the regulation of code.[9]

Our first claim is that coders will begin to encounter a regulation thicket, borrowing a concept from patent scholarship.[10] Given the intrinsic malleability of code, every coding endeavor will implicate a growing number of regulations, subjecting coders to a complex and entangled set of requirements, prohibitions, and obligations.

Our second claim is that agencies will run headlong into new conflicts with other agencies and with newly uncovered jurisdictional overlaps involving software, thus surfacing unresolved tensions and competing policy priorities.[11] For example, in 2015, privacy law watchers fretted about collisions between the FCC and FTC as the FCC began to expand its privacy enforcement activity. The FTC reclassified telecommunications systems (subject to privacy regulations) to include broadband internet service providers, treading onto ground cultivated and firmly held by the FCC.[12] A Memorandum of Under-

---

5 See *infra* Section I.D.

6 By "tinkerer," we mean a person who might traditionally have studied, taken apart, tweaked, and reassembled hardware systems in a hobbyist or professional capacity and who might now undertake the same or similar tasks with code.

7 Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (codified as amended in scattered sections of 17 U.S.C.).

8 *See infra* Section I.C.

9 *See infra* Part II.

10 *Cf.* Carl Shapiro, *Navigating the Patent Thicket: Cross Licenses, Patent Pools, and Standard Setting*, *in* 1 INNOVATION POLICY AND THE ECONOMY 119, 120 (Adam B. Jaffe et al. eds., 2000). For our discussion of the regulation thicket, see *infra* Section III.A.

11 See *infra* Section III.B.

12 *See* Jedidiah Bracy, *FTC Officials Concerned About Jurisdiction After FCC Net Neutrality Order*, IAPP: THE PRIVACY ADVISOR (Mar. 10, 2015), https://iapp.org/news/a/ftc-officials-concerned-about-jurisdiction-after-fcc-net-neutrality-order/ [https://perma.cc/6TBP-LAAT]. *See generally* Fed. Trade Comm'n v. AT&T Mobility LLC, No. 15-16585, 2016 WL 4501685 (9th Cir. Aug. 29, 2016).

standing[13] between enforcers in the two agencies ended the immediate hand-wringing, but its vague and open language raised questions about whether the Memorandum is less a peace treaty and more a cease-fire in this turf war.[14]

We offer a few prescriptions about how to deal with the problems that might arise from the increased regulation of code. We think the federal government should consider a centralized approach to at least some of the questions of code regulation. Perhaps a single agency—already in existence or yet to be created—can track and coordinate the regulation of code across the government as well as confront the new challenges posed by the transition of regulating software-based objects. It might also help agencies speak with one voice on difficult and recurring questions that might arise, such as how to define authorization or how to incorporate software design principles into solutions. At a bare minimum, the government might anticipate foreseeable conflicts and conceive of procedural mechanisms to resolve them.

Our analysis proceeds in four parts. Part I documents parallel shifts from hardware to software and from regulating things to regulating code, then explains why this shift matters. Part II offers a taxonomy for code regulation. Part III highlights problems that might arise from the shift. And finally, Part IV offers an argument for centralizing some (but not all) aspects of code regulation.

I. From Regulating Hardware to Software

Regulators who regulate hardware today will regulate software tomorrow because various industrial and economic trends are converting much activity from hardware to software. In this Part, we explore some root causes and empirical evidence of this shift. We then recount a pair of case studies from 2015 that heralded the shift. This shift matters, however, only if the distinction between hardware and software matters, and we point to a few reasons to believe that it does.

---

13 FCC-FTC Consumer Protection Memorandum of Understanding (Nov. 16, 2015), https://www.ftc.gov/system/files/documents/cooperation_agreements/151116ftcfcc-mou.pdf.

14 *See, e.g.*, Margaret Harding McGill, *Collaboration, Not Rivalry, Key in New FTC-FCC Pact*, Law360 (Nov. 19, 2015, 1:44 PM), http://www.law360.com/articles/728987/collaboration-not-rivalry-key-in-new-ftc-fcc-pact [https://perma.cc/KR6V-KPZB] (indicating that the agencies will endeavor to coordinate, but may both still exercise authority over the same matter when there is overlap).

A. *Atoms to Bits*

While law and policy often embed assumptions about whether a particular problem will be solved with hardware or software, computer scientists advance the "Principle of Equivalence of Hardware and Software."[15] Put simply, any computational task can be solved using either hardware or software or a combination of the two.[16] Where hardware ends and software begins in any given system depends on economic choices about the availability and allocation of resources, such as manufacturing, expertise, and other systems that may serve as foundations, not solely on the nature of the problem being solved.[17]

A society-wide and rapid shift is occurring from consumer goods, machines, and other devices implemented with noncomputational hardware to similar devices where hardware functionality is supplemented with, or in some cases entirely replaced by, software. Any system that embeds logic, broadly defined, is a candidate for a shift from hardware to software. Such systems range from the mechanical systems of an automobile to the diagnostics systems in medical devices and beyond. This matters to regulation only if there is something different about the regulation of hardware or software, a topic addressed in Section I.E. For now, consider some empirical evidence for this shift, some potential root causes, and the way this relates to the rise of the so-called Internet of Things.[18]

B. *Understanding the Shift*

Economists Mikko Packalen and Jay Bhattacharya elegantly summarize an important shift in American innovation: the shift from "atoms to bits."[19] The pair studies "new idea inputs" in invention by analyzing the text found in granted American patents, sorting these ideas by decade.[20] The early decades of the twentieth century are

---

15 LINDA NULL & JULIA LOBUR, THE ESSENTIALS OF COMPUTER ORGANIZATION AND ARCHITECTURE 3 (2003).

16 *Id.*

17 *See id.* at 2.

18 *See infra* notes 35–37 and accompanying text.

19 *See* Derek Thompson, *"From Atoms to Bits:" A Brilliant Visual History of American Ideas*, ATLANTIC (Feb. 9, 2015), http://www.theatlantic.com/business/archive/2015/02/a-short-history-of-american-invention/385279/ [https://perma.cc/SU96-6GPJ]; Mikko Packalen & Jay Bhattacharya, *New Ideas in Invention* 4–7 (Nat'l Bureau of Econ. Research, Working Paper No. 20922, 2015), http://www.nber.org/papers/w20922.pdf.

20 Packalen & Bhattacharya, *supra* note 19, at 5–6, Tbl. 1.

dominated by electrical and chemical ideas.[21] In the 1910s, for example, the five leading terms were "catalyst," "capacitance," "aircraft," "radio frequency," and "automotive."[22] The 1980s is the decade of computer hardware, drugs, and medical ideas, spurring terms "EEPROM," "hard disk drive," "network LAN," "laptop," "area network," "DNA sequence," "monoclonal antibodies," "expression vectors," and "gene expression."[23] But by the first decade of the twenty-first century, the twenty most popular new idea inputs all related to computers and communications, including "bluetooth," "markup language," "VoIP," "storage area network," and "instant messaging."[24]

The results this study demonstrates for American invention have also happened to American regulation. Where once we regulated mechanical objects or chemical reactions, we now regulate information systems that reach the same results. We do not mean analogically similar things; we mean precisely the same thing.

For example, wireless communication functionality was once performed by dedicated transmission and receiving devices—purpose-built by manufacturers and tightly regulated by the FCC—but is now performed by programmable, software-defined radios that can be configured for a variety of purposes—including some illegal purposes that were architecturally excluded when the FCC needed only to contend with regulating the manufacture of hardware.[25] Environmental pollution controls for automobiles, originally realized through devices physically installed on vehicles, are now realized through complex rules and algorithms built into software that controls the operation of modern engines.[26] Even medical devices like insulin controls and pacemakers increasingly have their operations controlled by software—so their safety features, too, must now rely on programming.[27]

---

21 *Id.*

22 *Id.*

23 *Id.*

24 *Id.*

25 *See generally* Friedrich K. Jondral, *Software-Defined Radio—Basics and Evolution to Cognitive Radio*, 3 EURASIP J. ON WIRELESS COMM. & NETWORKING 275 (2005) (providing an overview of the development of software-defined radio systems).

26 *See* Robert Wall, *How Car Software Can Rig a Test; A Complex Mix of Sensors, Engine-Management Software Track Emissions*, WALL ST. J. (Sept. 23, 2015, 12:24 PM), http://www.wsj.com/articles/auto-software-in-focus-after-volkswagen-flap-1442945494 [https://perma.cc/9G59-8DLZ].

27 Tom Haigh & Carl Landwehr, *Building Code for Medical Device Software Security*, IEEE CYBERSECURITY 4–6 (2015), http://www.computer.org/cms/CYBSI/docs/BCMDSS.pdf.

What is causing the shift from hardware to software? A complete account is beyond the scope and purpose of this Article, but consider one important root cause: the rise of the "end-user microprocessor." As recently as a decade ago, putting brains into a physical device required a set of esoteric skills.[28] Microprocessors—computer-processing chips—often required expensive special hardware to program and design, which limited the number of people who could do so.[29] The microprocessors available were underpowered, too large to squeeze into small consumer devices, and required many ancillary components to operate.[30] Advances in chip design enabled manufacturers to create more powerful and more self-contained processing onto a single chip and allowed them to do so for a fraction of the earlier cost.[31] This gave rise to "system on a chip" designs and new microprocessor systems such as the Arduino and Raspberry Pi.[32]

Today, it is very easy and relatively inexpensive to build a device with these systems. What once required an EEPROM burner, logic analyzer, and special training (not to mention a soldering iron) now can be done with a personal computer, a USB cable, and easy-to-use computer programming languages.[33] This dovetailed with, or maybe even helped give rise to, the Maker movement, which emphasizes do-it-yourself construction of electronics and other engineering pursuits.[34]

The shift from hardware to software has given rise to the so-called Internet of Things.[35] A defining characteristic of the Internet of Things is the proliferation of microprocessors into the physical world, where they run code.[36] At this current moment in time, the race is on

---

28 *See* Kenneth Leung, *A History of the Arduino Microcontroller* 3–4 www.KENLEUNG.CA, http://www.kenleung.ca/_portfolioassets/PDF/HistoryOfArduino_KenLeung.pdf.

29 *See id.* at 2.

30 *See id.*

31 *See id.* at 3.

32 *See id.*

33 See Evgeny Morozov, *Making It*, NEW YORKER (Jan. 13, 2014), http://www.newyorker.com/magazine/2014/01/13/making-it-2 [https://perma.cc/PT92-4RLB].

34 Id.

35 *See* Julie Brill, *The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control*, 83 FORDHAM L. REV. 205, 205–08 (2014); Meg Leta Jones, *Privacy Without Screens & the Internet of Other People's Things*, 51 IDAHO L. REV. 639, 641–42 (2015); Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 88–89 (2014); *see also* FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, STAFF REPORT 5–6 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

36 FTC, *supra* note 35, at 5 (surveying definitions of "Internet of Things" but noting that "there is still no widely accepted definition").

to stick these microprocessors into everything, from refrigerators to clothing to humans.[37]

Many of the devices now being equipped with microprocessors have historically been the subject of regulatory measures, which have had laudable goals—facilitating safety, preventing injury, ensuring security, reducing energy consumption and pollution, preventing wireless interference, and so forth. But these regulatory measures, previously targeted at devices themselves, must now directly contend with the software that operates the devices.

C. Case Studies

Consider the following two case studies that demonstrate the shift from hardware to software. The FCC's statutory instruction to police wireless spectrum interference formerly involved devices made of hardware (transmitters and receivers) for the most part but today often involves the regulation of software-defined radio.[38] Similarly, the most recent DMCA triennial review, completed in 2015, involved software-enabled devices in a breathtakingly large range of industrial activity, from cars and tractors to insulin pumps.[39] The latest review also drew in an eclectic cast of government agencies weighing in on (and perhaps weighing down) the process for the first time.[40]

1. The FCC Meets Open Firmware

Congress has long empowered the FCC to regulate wireless spectrum interference. This power is embodied in section 333 of the Communications Act of 1934,[41] which currently provides: "[n]o person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this chapter or operated by the United States Government."[42]

Before recent developments, policing section 333 meant policing hardware. People interfered with wireless bands allocated to another person or entity primarily by building homemade radios configured in

---

37 Peppet, *supra* note 35, at 88; *see also* Brill, *supra* note 35, at 206–07.

38 *See* Julius Knapp, *Securing RF Devices Amid Changing Technology*, FCC BLOG (Oct. 8, 2015, 3:56 PM), https://www.fcc.gov/news-events/blog/2015/10/08/securing-rf-devices-amid-changing-technology [https://perma.cc/5762-PUBD].

39 *See infra* notes 72–75.

40 *USCO Letters to Other Agencies*, U.S. COPYRIGHT OFFICE, http://copyright.gov/1201/2015/USCO-letters/ [https://perma.cc/Z2NS-YH4C] (last visited Oct. 3, 2016) (collecting letters both to and from other agencies during section 1201 review).

41 47 U.S.C. § 333 (2012).

42 *Id.*

a way that produced an interfering signal.[43] A complementary statute, section 302a(a),[44] affords the FCC the ability to promulgate regulations:

> (1) governing the interference potential of devices which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications; and (2) establishing minimum performance standards for home electronic equipment and systems to reduce their susceptibility to interference from radio frequency energy. Such regulations shall be applicable to the manufacture, import, sale, offer for sale, or shipment of such devices and home electronic equipment and systems, and to the use of such devices.[45]

The rise of so-called software-defined radio ("SDR"), however, changed wireless interference into a software game. An SDR is a hardware device designed to be able to be reconfigured quickly and using software alone.[46] With SDR, a user can use software to change, among other things, the frequency bands on which an SDR transmits and receives and the power output of its transmissions.[47] Each of these changes can raise the prospect of seamless and widespread new interference to other spectrum users.

Following the rise of SDRs, the question of how the FCC would adapt its section 333 responsibility came to a head with a document released in March 2015 by the FCC's Office of Engineering and Technology, Laboratory Division entitled *Software Security Requirements for U-NII Devices*.[48] U-NII stands for "Unlicensed National Information Infrastructure" and refers to devices that operate in the unli-

---

43 *See e.g.*, *Jammer Enforcement*, FCC, https://www.fcc.gov/general/jammer-enforcement [https://perma.cc/ZE4F-4BD4] (last visited Oct. 3, 2016); *see also* Thomas H. White, *Building the Broadcast Band*, U.S. EARLY RADIO HIST. (June 7, 2008), http://earlyradiohistory.us/buildbcb.htm.

44 47 U.S.C. § 302a(a).

45 *Id.*

46 *FCC Rules on FOSS and Software-Defined Radio*, SOFTWARE FREEDOM L. CTR., § 2.1 (July 6, 2007), https://www.softwarefreedom.org/resources/2007/fcc-sdr-whitepaper.html; *see also, e.g.*, Gregory Staple & Kevin Werbach, *The End of Spectrum Scarcity*, IEEE SPECTRUM (Mar. 1, 2004, 3:16 PM), http://spectrum.ieee.org/telecom/wireless/the-end-of-spectrum-scarcity [https://perma.cc/J9HW-6HQE].

47 *FCC Rules on FOSS and Software-Defined Radio*, *supra* note 46.

48 FCC Office of Eng'g & Tech. Lab. Div., *Software Security Requirements for U-NII Devices* (Mar. 18, 2015), https://assets.documentcloud.org/documents/2339685/fcc-software-security-requirements.pdf [hereinafter March FCC Memo].

censed 5 GHz band, which includes some Wi-Fi routers.[49] The short memo discusses the need for devices operating in this band to "reduc[e] the potential for harmful interference to authorized users" and its significant attendant consequences.[50]

The problem is that a community of programmers, tinkerers, and users has arisen around wireless routers, which are merely low-end computers with useful and specialized networking hardware built-in.[51] Two notable efforts are the DD-WRT[52] and OpenWRT[53] groups, both of which consist of coders creating new versions of the operating system for certain routers that include various types of increased functionality.[54]

Many in the community saw the March 2015 memo as a shot across their bow.[55] In fact, the memo lists DD-WRT by name, instructing router manufacturers to "[d]escribe in detail how the device is protected from . . . the installation of third-party firmware such as DD-WRT."[56] While the FCC clarified that it was intending to address only the impacts of the software on interference, the community saw it as a broader intrusion into their ability to tinker with all the software on the router, including applying security patches, enhancing functionality, and so forth.[57]

After public outcry, the FCC responded by amending the March 2015 memo in November 2015.[58] The revised memo deletes some of the sentences that most concerned the community, namely, those which sought to require manufacturers to "prevent third parties from loading [certain] versions of the software/firmware on the device" and

---

49 *Id.* at 1.

50 *Id.*

51 Bradley Mitchell, *Router*, ABOUT TECH., http://compnetworking.about.com/cs/routers/g/bldef_router.htm (last updated Oct. 3, 2016).

52 *DD-WRT Privacy: Regain Your Internet Freedom*, DD-WRT.COM, http://www.dd-wrt.com/site/dd-wrt_privacy [https://perma.cc/J6TY-F4UQ] (last visited Aug. 7, 2016).

53 *What is OpenWrt?*, OPENWRT, http://openwrt.org (last visited Oct. 3, 2016).

54 *See supra* notes 52–53.

55 Jon Brodkin, *FCC: We Aren't Banning DD-WRT on Wi-Fi Routers*, ARS TECHNICA (Nov. 12, 2015, 1:50 PM), http://arstechnica.com/information-technology/2015/11/fcc-we-arent-banning-dd-wrt-on-wi-fi-routers/ [https://perma.cc/6V9J-W788]; Rob Marvin, *FCC Fires Wi-Fi Router Salvo in Battle of DRM vs. Open Source*, PCMAG.COM (Sept. 2, 2015, 1:10 PM), http://www.pcmag.com/article2/0,2817,2490525,00.asp [https://perma.cc/Q7RG-LV7C].

56 March FCC Memo, *supra* note 48, at 2.

57 *See* Brodkin, *supra* note 55.

58 FCC Office of Eng'g & Tech. Lab. Div., *Software Security Requirements for U-NII Devices* (Nov. 12, 2015), https://apps.fcc.gov/kdb/GetAttachment.html?id=zXtrctoj6zH7oNEOO6De6g%3D%3D&desc=594280%20D02%20U-NII%20Device%20Security%20v01r03&tracking_number=39498 [hereinafter November FCC Memo].

those singling out DD-WRT as a specific example.[59] In their place, it asks device manufacturers to

> [d]escribe, if the device permits third-party software or firmware installation, what mechanisms are provided by the manufacturer to permit integration of such functions while ensuring that the RF parameters of the device cannot be operated outside its authorization for operation in the U.S. In the description include what controls and/or agreements are in place with providers of third-party functionality to ensure the devices' underlying RF parameters are unchanged and how the manufacturer verifies the functionality.[60]

This new language accomplishes two important goals. First, it abandons the implicit advice about "prevent[ing]" third-party firmware to a more neutral one of acknowledging that some manufacturers might permit third-party firmware (but it perhaps disappoints those who wanted the FCC to go further and affirmatively encourage open hardware instead). Second, the new memo focuses on "RF parameters" as the sole area of concern for the FCC, implying that firmware developers can let their users configure other aspects of their software.[61]

This case study exemplifies one dynamic that can result from the shift from hardware to software: the unintended consequences of applying hardware-specific regulations to software that will likely interact with those regulations in new and unpredictable ways.

2. The 2015 DMCA Triennial Review

The 2014–2015 triennial review of exemptions to section 1201 of the DMCA conducted by the Library of Congress and U.S. Copyright Office ultimately found that users, coders, tinkerers, researchers, manufacturers, the Copyright Office, the EPA, the FDA, and the National Telecommunications & Information Administration ("NTIA") are locked in a battle over the legality of tinkering with, hacking, and researching cars, tractors, planes, voting machines, cryptography systems, electronic baby toys, and more. How did a statute ostensibly focused on copyright lead to such a result?

First, some background on section 1201. The statue was originally designed to help facilitate the secure distribution of digital content—mainly video programming—by making it illegal to circumvent

---

59 *See* March FCC Memo, *supra* note 48, at 2.

60 November FCC Memo, *supra* note 58, at 2–3.

61 *Id.*

digital locks (popularly, "digital rights management" ("DRM") or in the statute's parlance, "technological protection measures" ("TPMs")) on that content or to develop and distribute tools to do so.[62] However, section 1201 makes illegal the circumvention of (and the development and distribution of tools for circumventing) TPMs placed on any copyrighted work—including computer software.[63]

Thus, as computer software has pervaded more and more everyday devices over the past two decades, section 1201 has increasingly become viewed by some not simply as a narrow copyright statute, but as a more general statute regulating the circumvention of computer code with security features.[64] This development has occurred organically and without specific legislative or administrative intervention. This is because section 1201 regulates circumvention and tool development and distribution *by default*, leaving consideration of temporary (three-year) *exemptions* to a triennial review conducted by the Library of Congress and the Copyright Office.[65]

During each triennial review, the Copyright Office reviews a variety of proposals from various stakeholders to grant exemptions for circumvention under certain circumstances and therefore must effectively make a decision about whether to continue banning circumvention in those contexts.[66] During the 2014–2015 review, a flurry of exemption requests were submitted involving computer code:

- A cohort of "unlocking" exemptions, aimed at permitting modifying baseband firmware on smartphones, tablets, and other devices to move them from one cellular network to another.[67]
- Several "jailbreaking" exemptions, aimed at modifying locks on smartphones, ebook readers, video game consoles, smart TVs, and other devices to install applications not approved by the devices' manufacturers.[68]

---

62 *See* 17 U.S.C. § 1201(a)–(b) (2012).

63 *See id.* §§ 102, 1201(a)–(b).

64 *See* Parker Higgins, *EFF to Congress: Get Rid of DMCA's "Anti-Circumvention" Provisions*, ELEC. FRONTIER FOUND. (Sept. 17, 2014), https://www.eff.org/deeplinks/2014/09/eff-congress-get-rid-dmcas-anti-circumvention-provisions [https://perma.cc/4W9P-UUGZ].

65 *See* 17 U.S.C. § 1201(a)(1)(C)–(D).

66 *See id.*

67 *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 79 Fed. Reg. 73,856 (proposed Dec. 12, 2014) (to be codified at 37 C.F.R. pt. 201) [hereinafter Exemption to Prohibition]; *see also, e.g.*, Competitive Carriers Association, *Petition for Proposed Exemption Under 17 U.S.C. § 1201*, U.S. COPYRIGHT OFFICE, LIBRARY OF CONG., http://copyright.gov/1201/2014/petitions/Competitive_Carriers_Association_3_1201_Initial_Submission_2014.pdf.

68 *See* Exemption to Prohibition, *supra* note 67; *see also, e.g.*, Comments of Electronic

- A pair of exemptions focused on circumvention of TPMs on software installed on vehicles, including both cars and farm equipment—one for security and safety research and the other for diagnosis, repair, or modification.[69]
- An exemption focused on circumvention of TPMs on software for networked medical devices, such as insulin pumps, aimed at both safety and security and allowing patients to extract health data about themselves.[70]
- Several proposed exemptions around security research on a variety of computer systems.[71]

The proposed vehicle, medical, and computer security exemptions prompted extensive discussion during the rulemaking around policy matters bearing little relation to copyright law. For example:

- The vehicle exemptions prompted discussion around the extent to which the modification of vehicle software could result in violations of the EPA's emissions standards and various traffic safety laws.[72]
- The medical exemption prompted discussion around the extent to which accessing the software on medical devices was consistent with the FDA's regulation of the cybersecurity of medical devices and health privacy law.[73]

Frontier Foundation and Organization for Transformative Works, Docket No. 2014-07, before the U.S. Copyright Office, Library of Cong., http://www.copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_EFFOTW_Class07.pdf.

69 *See* Exemption to Prohibition, *supra* note 67; *see also, e.g.*, Elec. Frontier Found., Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. 2014-07, before the U.S. Copyright Office, Library of Cong., http://copyright.gov/1201/2014/petitions/Electronic_Frontier_Foundation_1201_Initial_Submission_2014.pdf.

70 *See* Exemption to Prohibition, *supra* note 67; *see also, e.g.*, Berkman Ctr. for Internet & Soc'y, Petition of a Coalition of Medical Device Researchers for Exemption to Prohibition of Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. 2014-07, before the U.S. Copyright Office, Library of Cong., http://copyright.gov/1201/2014/petitions/Berkman_Center_1201_Initial_Submission_2014.pdf.

71 *See* Exemption to Prohibition, *supra* note 67; *see also, e.g.*, Matthew Green, *Short Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201*, U.S. COPYRIGHT OFFICE, LIBRARY OF CONG., http://www.copyright.gov/1201/2015/comments-020615/InitialComments_shortform_MGreen_Class22.pdf.

72 U.S. COPYRIGHT OFFICE, LIBRARY OF CONG., SIXTH TRIENNIAL 1201 RULEMAKING HEARINGS 26, 35, 144 (May 26, 2015); *see also* U.S. COPYRIGHT OFFICE, SECTION 1201 RULEMAKING: SIXTH TRIENNIAL PROCEEDING TO DETERMINE EXEMPTIONS TO THE PROHIBITION ON CIRCUMVENTION: RECOMMENDATION OF THE REGISTER OF COPYRIGHTS 267 (2015) [hereinafter U.S. COPYRIGHT OFFICE, RECOMMENDATION OF THE REGISTER].

73 U.S. COPYRIGHT OFFICE, LIBRARY OF CONG., *supra* note 72, at 33–36, 133–34, 144; *see also* U.S. COPYRIGHT OFFICE, RECOMMENDATION OF THE REGISTER, *supra* note 72, at 276.

- The security exemption prompted discussion around the extent to which security research might pose risks to public safety—including a recent episode involving hacking of an airplane's avionics system—or inspire violations of the Computer Fraud and Abuse Act ("CFAA"),[74] and also included discussion regarding the appropriate policy for requiring researchers to report security risks to responsible companies before reporting them to the public.[75]

Ignoring pleas from exemption proponents to stay focused on copyright policy issues, the Copyright Office took the unprecedented step of soliciting feedback on the exemptions from the EPA, the FDA, the Department of Transportation ("DOT"), and the National Highway Traffic Safety Administration ("NHTSA").[76] The responses varied:

- The EPA urged the Copyight Office to deny the vehicle exemptions on the grounds that they would facilitate the practice of modifying vehicles to exceed the emissions limits in the Clean Air Act.[77]
- The DOT expressed concern that the vehicle exemptions could facilitate violations of the National Traffic and Motor Vehicle Safety Act and thus urged the Copyright Office to adopt disclosure limitations on information gleaned from vehicle security research that is enabled by the vehicle security exemption.[78]
- The FDA took a less aggressive view, urging the Copyright Office to make clear that an exemption from section 1201 would not affect obligations of circumventors under the Federal Food, Drug, and Cosmetic Act.[79]

---

74 Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (2012).

75 U.S. COPYRIGHT OFFICE, LIBRARY OF CONG., *supra* note 72, at 125–51; *see also* U.S. COPYRIGHT OFFICE, RECOMMENDATION OF THE REGISTER, *supra* note 72, at 312–15.

76 *USCO Letters to Other Agencies*, *supra* note 40 (collecting letters both to and from other agencies during § 1201 review).

77 Letter from Geoff Cooper, Assistant General Counsel, U.S. Envtl. Protection Agency, to Jacqueline C. Charlesworth, General Counsel and Associate Register of Copyrights, U.S. Copyright Office, Library of Cong. (July 17, 2015) (http://copyright.gov/1201/2015/USCO-letters/EPA_Letter_to_USCO_re_1201.pdf).

78 Letter from Kathryn B. Thomson, General Counsel, U.S. Dep't of Transp., to Jacqueline C. Charlesworth, General Counsel and Associate Register of Copyrights, U.S. Copyright Office, Library of Cong. (Sept. 9, 2015) (http://copyright.gov/1201/2015/USCO-letters/DOT_Letter_to_USCO_re_1201.pdf).

79 Letter from Bakul Patel, Associate Dir. for Digital Health Ctr. for Devices and Radiological Health, Food & Drug Admin., U.S. Dep't of Health & Human Servs., to Jacqueline C. Charlesworth, General Counsel and Associate Register of Copyrights, U.S. Copyright Office,

Suddenly, the Copyright Office found itself at the center of a full-fledged, multiagency debate over the extent to which code regulation might be necessary not just for copyright policy reasons, but for environmental, traffic, health, and various other noncopyright policy reasons as well.[80]

The NTIA, with which section 1201 obliges the Copyright Office to consult in considering exemptions,[81] blasted the Office for going too far.[82] The NTIA noted that the triennial review had "stood out for its extensive discussions of matters with no or at best a very tenuous nexus to copyright protection," and criticized the Office for trying to "develop expertise in every area of policy that participants may cite on the record."[83] The NTIA urged the Office not to "heavily weigh unrelated matters such as greenhouse gas emissions or the quality of materials used to build aircraft, and . . . instead [to] focus primarily on questions relevant to copyright law," noting that "Congress, applicable regulatory agencies, and their counterparts within state governments are well-equipped to deal with these non-copyright issues in the appropriate settings and under legal authorities focused on those issues."[84]

This case study exemplifies a different dynamic from the FCC/SDR example: the complex and interconnected suite of policy issues, values, and law that will often arise when an agency tries to regulate hardware that has shifted to incorporate software.

D. Looking Ahead

We think that the FCC/SDR and DMCA examples are just the beginning. With every passing year, and as more human and industrial activity shifts from hardware to software, more government agencies will find themselves pressed—some willingly, some kicking and screaming—into regulating software. Consider only a few additional

---

Library of Cong. (Aug. 18, 2015) (http://copyright.gov/1201/2015/USCO-letters/FDA_Letter_to_USCO_re_1201.pdf).

80 *See USCO Letters to Other Agencies*, *supra* note 40; U.S. COPYRIGHT OFFICE, RECOMMENDATION OF THE REGISTER, *supra* note 72, at 312–15.

81 17 U.S.C. § 1201(a)(1)(C) (2012).

82 *See* Letter from Lawrence E. Strickling, Assistant Sec. for Commc'ns & Info., Nat'l Telecomm. & Info. Admin., U.S. Dep't of Commerce, to Maria A. Pallante, Register of Copyrights, Library of Cong., attachment at 5 (Sept. 18, 2015), http://copyright.gov/1201/2015/2015_NTIA_Letter.pdf [hereinafter NTIA Letter].

83 *Id.* at 3–4.

84 *Id.* at 5.

examples from 2015 that demonstrate the increasing engagement of agencies with software.

EPA v. VW. The revelation that Volkswagen had devised software in millions of automobiles that could switch on environmental control systems only during emissions testing has already become a centerpiece in debates over the regulability of code.[85] We are sure that this story will be retold and analyzed by legal scholars for years, if not decades, to come. We focus on it for only a small part of this story: the EPA, an agency charged with understanding the intricacies of catalytic converters, dynamometers, and other physical devices, must now understand complex software processes that are integrated with those physical devices.

FDA and Medical Devices. The FDA has long been charged with ensuring the safety of medical devices, including those implanted in patients, such as pacemakers and insulin pumps.[86] However, those devices have increasingly begun to include complex software stacks, such as wireless networking protocols that raise serious concerns about the security of those devices.[87] This dynamic has led the FDA to regulate the manufacturers of medical devices that include software and additionally to opine when others seek to interact with the code on devices, including independent researchers and even patients.[88]

FAA and Drones. The FAA has, of course, regulated software for decades. Long before the Copyright Office or the FDA thought about software, the FAA was worried about the software routines in airplanes, airports, air traffic centers, and, beyond that, superintended flight operations, safety, air traffic, and more.[89]

It still seems, however, that the FAA, despite its historical experience with software regulation, has seen a shift in focus, at least in degree if not in kind. Suddenly, the FAA has been asked to police

---

85 *See, e.g.*, Megan Geuss, *US Sues Volkswagen over Defeat Device Scandal*, Ars Technica (Jan. 4, 2016, 3:25 PM), http://arstechnica.com/cars/2016/01/us-sues-volkswagen-over-defeat-device-scandal/ [https://perma.cc/E3R5-23JD].

86 William H. Maisel, *Medical Device Regulation: An Introduction for the Practicing Physician*, 140 Annals Internal Med. 296, 296 (2004).

87 *See* Food & Drug Admin., Postmarket Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff (Jan. 22, 2016), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf.

88 *Id.*

89 *See* Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544, 9544 (notice of proposed rulemaking Feb. 23, 2015) (to be codified at 14 C.F.R. pts. 21, 43, 45, 47, 61, 91, 101, 107, 183).

airspace abuzz (quite literally) with thousands of very cheap drones.[90] Unlike the airplanes that have been the object of the FAA's regulatory attention for a century, these devices are manufactured by small start-up companies—including toy manufacturers—without a history of regulatory scrutiny. Moreover, they are being operated and modified by average citizens with no formal training.[91]

NHTSA and Connected Cars. One final example of an agency suddenly forced to think about software in new ways is the NHTSA. This small subagency within the DOT has been asked to investigate software in automobiles—not only the consumer-facing interfaces in connected cars, for example, but also in the systems controlling vehicles themselves.[92]

E. Why This Matters

We think the shift from hardware to software matters because agencies will find their traditional approaches to regulation at least disrupted—if not entirely upended—when the object of their attention shifts. This is a contestable claim, and we do not prove it here definitively. Whether regulating software is different in kind or merely in degree from regulating hardware, and, if only in degree, the size of the change, are questions that deserve to be studied in greater depth than we present here.

In this Article, it will suffice to point to some reasons why the hardware-to-software transition is important and difficult. At the core of the importance and difficulty is the fact that hardware and software differ in several important ways. Most importantly, software evolves and changes more quickly than hardware.[93] Jonathan Zittrain's theory of generativity explains why: software is easier to change and customize than hardware.[94]

---

90 *Id.*

91 *See, e.g.*, Paul Stamatiou, *Getting Started with Drones*, PAULSTAMATIOU.COM (July 30, 2014), http://paulstamatiou.com/getting-started-with-drones-quadcopters/ [https://perma.cc/M7PN-BZ2Y] (teaching beginners the basics of learning to use and modify drones).

92 NHTSA, U.S. DEPT. OF TRANS., FEDERAL AUTOMATED VEHICLES POLICY: ACCELERATING THE NEXT REVOLUTION IN ROADWAY SAFETY (2016); Rachael King, *Automakers Tackle the Massive Security Challenges of Connected Vehicles*, WALL ST. J. BLOG: CIO J. (June 25, 2015, 3:10 PM), http://blogs.wsj.com/cio/2015/06/25/automakers-tackle-the-massive-security-challenges-of-connected-vehicles/ [https://perma.cc/KKW4-TPV8].

93 *See* JONATHAN L. ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 15 (2008) (noting that while a PC's hardware does not change, the processing software may be repeatedly upgraded or replaced).

94 *Id.*

As the VW example highlights, software is also easier to obscure. Software systems can be turned on or off through the simple application of a few lines of code, in contrast to hardware systems that may require cumbersome and visible physical modifications to facilitate the same operation.[95] Software code can be buried in binary code and tamper-proof chips and can even be encrypted.[96] While many regulatory regimes rest on the presumption that a system's operation can be observed and verified, verifying that complex computer code operates in a particular way is both theoretically and practically difficult to perform at any degree of precision.[97]

For these reasons, we think the tools, personnel, and expertise developed slowly by agencies since the rise of the industrial revolution will not deal well with the software shift. Unfortunately, the generativity and obscurability of software means that an agency must do more than merely learn how to regulate software; the agency will quickly learn that software is a moving target not necessarily susceptible to legacy regulations. There are sure to be growing pains as agencies realize that their old methods and expertise may no longer work well, and there will be unintended consequences from the regulations that result from these challenging circumstances. In Part IV, we diagnose a few of these potential problems, and in Part V, consider a few ways to avoid the worst of them.

II. A Taxonomy of Code Regulation

The regulation of software will take many different forms and target many different types of activity. Accordingly, it might be useful to lend some structure to software regulation, and in this Part we propose a taxonomy. As with any such effort, we think there is more than one way to organize the regulation of software, but we think the taxonomy we have developed provides a straightforward framework, one we will use to develop prescriptions in the final Part of this Article.

Our taxonomy builds on three aspects of the laws we are considering. First, and most importantly, we separate laws by the types of activities engaged in by the people subject to the regulation, for example, coding, tinkering, or using software. Second, we look for distinc-

95 *See id.* at 4.

96 *See id.* at 248.

97 Yuji Kukimoto, *Introduction to Formal Verification*, Donald O. Peterson Ctr. for Elec. Systems Design (Feb. 6, 1996, 11:58 PM), https://embedded.eecs.berkeley.edu/research/vis/doc/VisUser/vis_user/node4.html.

tions by thinking about software system architecture. Some laws restrict their attention to particular points in the so-called network layers model—for example, laws that focus on application developers or infrastructure providers.[98] Alternatively, some laws draw different architectural lines, focusing, for example, on platforms or intermediaries.[99] Third, and finally, we draw some lines based on the manufacturing lifecycle of software, asking whether agencies should intervene during initial software development, during deployment, or in an after-market, post-manufacturing stage. To put these three considerations another way, we thought about the *who*, the *where*, and the *when* of software regulation.

One virtue of our taxonomy is its simplicity. We reduce software regulation into four major categories based on the target of regulation: coders, users, platforms, and security, with subcategories for the latter two. Despite the relatively few moving parts of this system, we contend that virtually every regulation that could fall under the label "software regulation" fits within one of these parts.

We also hope that the taxonomy's framework can contribute to the development of sound regulation. The lines between the four categories and six subcategories will likely be the same lines regulators will draw between approaches to regulation. In other words, a law regulating platforms will differ from one regulating coders in systematic and important ways. Regulators will understand better how to learn from other agencies using the taxonomy; they will be well-advised to pay closer attention to precedents from the same part of the taxonomy in which they dwell, and they will understand that precedents from across the taxonomy are less useful and perhaps irrelevant.

A. Coders

Our first category of software regulation focuses on coders. These laws and regulations regulate software developers directly. This is often because lawmakers suspect that certain types of software created by coders are likely to raise tricky or worrisome public policy issues.

For example, coders can be regulated to stop them from creating software deemed to infringe on copyrights in other software. In *Lotus v. Borland*,[100] for example, the creators of Lotus 1-2-3 sued a competi-

---

98 *See supra* Part I.

99 *See supra* Part I.

100 Lotus Dev. Corp. v. Borland Int'l, Inc., 49 F.3d 807 (1st Cir. 1995), *aff'd per curiam*, 516 U.S. 233 (1996).

tor, Borland, for allegedly developing software that took too much copyrighted expression.[101]

Another example is the law of export controls as applied to encryption software. Under the ITAR and its successors, the EAR and the Wassenaar Arrangement, government agencies including the Department of Commerce's Bureau of Industry and Security have scrutinized and sometimes blocked people from distributing software containing certain "strong" forms of encryption and cybersecurity software.[102]

B. Users

Many laws are directed at the users of software. For purposes of this taxonomy, we are distinguishing between software under the direct control of a user, which fits in this category, and software distributed on a platform, which we place in the next major category.[103]

Again, copyright law provides many important examples. The lawsuits against users of peer-to-peer networks of the early 2000s are prime examples.[104] In addition to suing the developers who created—and the corporations that hosted—services like Grokster, the recording industry targeted individual downloaders as well.[105] Another early and important example is the case *MAI Systems Corp. v. Peak Computer, Inc.*,[106] in which a computer repair firm was sued for using the licensed software of its customers as a result of its repair activity.[107]

C. Platforms

Many laws focus on software distributed via platforms. The decision to deliver software as services via the internet raises novel and challenging issues of law and policy. Within the platforms category, we perceive at least three subcategories, which we are calling: Platform/User, Platform/Platform, and Platform/Replacement.

---

101 *Id.* at 810.

102 Sean B. Hoar & Bryan Thompson, *Pardon the "Intrusion"—Cybersecurity Worries Scuttle Wassenaar Changes*, PRIVACY & SECURITY L. BLOG (Sept. 4, 2015), http://www.privsecblog.com/2015/09/articles/cyber-national-security/pardon-the-intrusion-cybersecurity-worries-scuttle-wassenaar-changes/ [https://perma.cc/6QCT-9JD6].

103 This distinction is increasingly likely to erode, particularly as more software becomes distributed via the cloud.

104 *See generally* Elec. Frontier Found., RIAA v. The People*: Five Years Later*, EFF.ORG (Sept. 30, 2008), https://www.eff.org/files/eff-riaa-whitepaper.pdf.

105 *See id.* § I.

106 MAI Systems Corp. v. Peak Comput., Inc., 991 F.2d 511 (9th Cir. 1993).

107 *Id.* at 517–19.

1. *Platform/User*

Some regulations focus on the users of platforms. Again, this category overlaps with the unadorned Users category above. We place this activity in a separate category, however, because we find recurring themes involving users of platforms that do not occur in earlier, direct-control cases.

Again, these regulatory efforts focus on a user who uses software in a disfavored way. From copyright, for example, we have the raft of notice-and-takedown actions brought against users of YouTube.[108] Like the lawsuits against users of Grokster, these actions targeted individuals, but because of the role played by the owner of the platform, there is more of a three-party dynamic at play—the content owner, the platform, and the user—suggesting the need for a distinct part of the taxonomy.

2. *Platform/Platform*

Rather than target the user of a platform, sometimes laws or regulations focus on the platform itself. In rare cases, these efforts label almost an entire platform as the site of unlawful activity; see, for example, *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*[109] or the actions against MegaUpload.[110] In addition, cases against platforms involve the notice-and-takedown provisions of the DMCA, which find a regulatory lever in the third-party platform.[111]

A key issue arising in Platform/Platform cases is statutory immunity, most importantly via section 230 of the Communications Decency Act.[112] This provision affords immunity to various types of platforms for illegal acts performed by platform users.[113]

3. *Platform/Replacement*

In recent years, regulatory attention has focused on a recurring pattern, one that has received much less scholarly commentary.

---

108 *E.g.*, Lenz v. Universal Music Corp., 801 F.3d 1126, 1129 (9th Cir. 2015) (holding that before sending a takedown notice, a copyright holder must consider the fair use doctrine in forming a good-faith belief that use of copyrighted material constitutes infringement of the copyright).

109 Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

110 *See* Kim Zetter, *Judge Rules Kim Dotcom Can Be Extradited to U.S. to Face Charges*, WIRED (Dec. 22, 2015, 5:50 PM), http://www.wired.com/2015/12/kim-dotcom-extradition-ruling/ [https://perma.cc/N6G5-L3KQ].

111 *See* 17 U.S.C. § 512 (2012).

112 47 U.S.C. § 230 (2012).

113 *See id.*

Sometimes, rather than using the entire platform developed by the platform designer, a community of users will replace the upper software layers of the platform with its own, custom-built software or firmware.[114] These users are able to do this by taking advantage of at least three related phenomena: general purpose computing, the generativity of platforms, and layered design principles.

A hacker community has engaged in jailbreaking or rooting of smartphones.[115] Sometimes, this activity is restricted to removing some of the security of these devices to enable the installation of software outside the strictures of the official app store.[116] In other cases, a community will completely replace the entire operating system of the phone, creating what seems like an entirely new product.[117] In successive DMCA exemption proceedings, the Librarian of Congress has granted exemptions for some forms of jailbreaking.[118]

Similarly, a separate community has focused on creating firmware for embedded devices, most notably wireless routers.[119] This is the community that has raised eyebrows at the FCC, because they essentially can reprogram the flexible radio hardware in these routers to violate FCC interference laws.[120]

D. Security

The final category in our taxonomy is security. Unlike the first two categories, which focused on people (coders and users) and the third major category, platforms, which focused on architecture, this final category focuses on a recurring pattern of behavior. Security issues involve the designation of a protected/restricted "inside" of a computer network or system and a disfavored/excluded "outside." Many laws and policies, including the CFAA, the DMCA, and the HIPAA Security Rule,[121] bolster technical methods for security by using legal or regulatory solutions.

---

114 *See, e.g.*, Jenna Wortham, *Unofficial Software Incurs Apple's Wrath*, N.Y. TIMES (May 12, 2009), http://www.nytimes.com/2009/05/13/technology/13jailbreak.html.

115 *Id.*

116 *Id.*

117 Miguel Helft, *Meet Cyanogen, the Startup That Wants to Steal Android from Google,* FORBES (March 23, 2015, 9:00 AM), http://www.forbes.com/sites/miguelhelft/2015/03/23/meet-cyanogen-the-startup-that-wants-to-steal-android-from-google-2 [https://perma.cc/A6SA-CPUV].

118 Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 208, 65,944, 65,952 (Oct. 28, 2015) (to be codified at 37 C.F.R. pt. 201).

119 *See supra* Section I.C.1.

120 *See supra* Section I.C.1.

121 45 C.F.R. § 160 (2007).

As with the Platform category, we further subdivide Security into three subcategories: Security/Hackers, Security/Researchers, and Security/Blackboxes.

1. Security/Hackers

Some laws are designed to prevent outsiders from gaining access to a secured system.[122] These laws target those outsiders—or hackers, to follow the convention—by providing for legal sanction and other tools to prevent, detect, and deter hackers.

The CFAA is the primary example. It rests fundamentally on the concept of authorization, a concept given exacting scrutiny in other articles in this Symposium.[123] Other examples include the provisions of the DMCA that focus on users of circumvention tools and techniques.[124]

2. Security/Researchers

Some laws focus not only on the end-users who ultimately breach security but also on those who probe, research, or study a system, often for the purpose of finding flaws in the security system. Many of these researchers aim to develop tools to empower other users to circumvent the security.

We recognize that in many cases the only thing that distinguishes the hacker and the researcher is motive. We are unapologetic about this blurring, because we think that many important policy lines are drawn along this same blurred border. For example, many of the DMCA exemptions that have been granted in the triennial review process have turned on the status or motive of the person doing the circumvention.[125] Once again, both the DMCA and CFAA have been used against researchers.[126]

---

122 *See, e.g.*, 18 U.S.C. § 1030; 17 U.S.C. § 1201(a)(2)(b) (2012).

123 James Grimmelmann, *Consenting to Computer Use*, 84 GEO. WASH. L. REV. 1500 (2016); Josh Goldfoot & Aditya Bamzai, *A Trespass Framework for the Crime of Hacking*, 84 GEO. WASH. L. REV. 1477 (2016).

124 17 U.S.C. § 1201(b).

125 Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 208, 65,944, 65,952 (Oct. 28, 2015) (to be codified at 37 C.F.R. pt. 201) ("Proposed Classes 16 and 17: Jailbreaking—Smartphones and All-Purpose Mobile Computing Devices").

126 Matthew D. Green, Long-Form Comment: Proposed Class 25: Security Research, Docket No. 2014-07, before the U.S. Copyright Office, Library of Cong., at 18 http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_Green_Class25.pdf.

3. Security/Blackbox

Finally, some software regulation puts the regulator in the role of the circumventer or user. In these situations, the regulator desires to peer into the inner-workings of a complex system, and they are thwarted by security measures.[127] In many ways, these regulators are like the hacker facing a secure network or a copyright user facing DRM. They have been deemed "outsiders" by the security system, and they are attempting to find their way into the inside, at least for a peek.

Volkswagen's attempts to thwart scrutiny by environmental regulators are the best example to date of this form of software regulation.[128] In this example, environmental regulators were required in an enforcement posture to verify the operation of emission controls on Volkswagen's vehicles to determine whether they were operating properly.[129]

III. Implications and Challenges

As regulators turn their attention from hardware to code, we predict significant challenges. We focus on three. First, coders will find themselves the object of attention of multiple agencies, each espousing inconsistent or flatly contradictory rules or guidance.[130] This will give rise to a "regulatory thicket," which has the potential to slow the pace of innovation in some areas.[131] Second, regulators will engage in new forms of turf warfare with other regulators.[132] Without statutory amendment, the boundaries of each agency's jurisdiction will creep outward.[133] This will exacerbate competition and tension between agencies that already compete, such as the FCC and FTC, and it will create new tensions between pairs of agencies that have almost never before interacted, such as NHTSA and the FTC.[134]

---

127 *See, e.g.*, *EPA, California Notify Volkswagen of Clean Air Act Violations/Carmaker Allegedly Used Software that Circumvents Emissions Testing for Certain Air Pollutants*, EPA: Verity View (Sept. 18, 2015), https://www.epa.gov/newsreleases/epa-california-notify-volkswagen-clean-air-act-violations-carmaker-allegedly-used [https://perma.cc/L2NX-4KBU].

128 EPA, *Volkswagen Light Duty Diesel Vehicle Violations for Model Years 2009–2016*, http://www.epa.gov/vw (last updated June 28, 2016) (collecting government documents relating to violations).

129 *See id.*

130 *See infra* Section III.A.

131 *See infra* Section III.A.

132 *See infra* Section III.B.

133 *See infra* text accompanying note 142.

134 *See infra* text accompanying notes 143–49.

A. The Regulatory Thicket

Carl Shapiro famously described the rise of American patent law as a "patent thicket, a dense web of overlapping intellectual property rights that a company must hack its way through in order to actually commercialize new technology."[135] According to Shapiro, this might mean "stronger patent rights can have the perverse effect of stifling, not encouraging, innovation."[136]

The rise and spread of code regulation suggests that we may be witnessing the rise of a code regulation "thicket." Whether one is creating software from scratch, improving on another's code, or merely using a device that happens to have code running on it, one must worry about code as never before.

This dynamic is showcased in a number of the examples noted above. For example, the tinkerers who seek to replace the operating systems on their wireless routers may face multiple legal barriers to doing so.[137] Router modifications, for example, may run afoul of FCC regulations aimed at preventing harmful interference.[138] Steps taken to address the FCC's rules, however, may themselves require the circumvention of digital rights management technologies placed on the router firmware by the manufacturer, exposing the tinkerer to liability under the DMCA.[139]

Similarly, security researchers who attempt to probe and identify vulnerabilities may not only face liability under the CFAA (for accessing computer systems without authorization) and the DMCA (for circumventing technological protection measures on the systems' copyrighted computer code), but may be increasingly forced to endure scrutiny from other agencies, such as the EPA, FDA, or FAA, if their research strays into computer systems on cars and tractors, medical devices, or aircraft and drones.[140]

The analogy is not perfect. The number of agencies that might be focused on a particular type of software is unlikely to exceed double digits, even when state and foreign agencies are considered. The number of patents (not to mention patent claims) that might arguably

---

135 Shapiro, *supra* note 10, at 120.

136 *Id.*

137 *See* Brodkin, *supra* note 55.

138 *See id.*

139 *Cf.* Audrey Watters, *Sony and "Geohot" Settle PS3 Jailbreak Lawsuit*, READWRITE (Apr. 11, 2011), http://readwrite.com/2011/04/11/sony_and_geohot_settle_ps3_jailbreak_lawsuit [https://perma.cc/UY5M-RBYC] (discussing settlement of CFAA and DMCA lawsuit between Sony and creator of replacement firmware for Playstation 3).

140 *See supra* notes 66–84 and accompanying text.

cover a developer may be several orders of magnitude greater.[141] Still, we think the confusion and uncertainty created by agency concerns over software has a similar impact on developers, as did patent thickets, and that reformatory efforts to clear the path for activities like security research are likely to face similarly prohibitive difficulties. And the software regulation thicket is likely to get much worse as more agencies join in.

B. New Turf Wars

As the targets of regulation face an increasingly tangled thicket of regulation, regulators are likely to tangle with each other. As the recent DMCA triennial review underscored, regulators such as the Copyright Office and the DOJ, who have historical dominion over computer software and mandates to prevent copyright infringement and computer hacking, are likely to collide with agencies with both complementary and competing mandates.[142]

The EPA, for example, may seek to both prevent tinkerers from modifying vehicles to evade emissions protections through the use of software protections, while simultaneously relying on the help of independent researchers to test the security of those protections, and also to penetrate them to verify that manufacturers of the underlying software are complying with emissions protections. The FDA may seek to prevent malicious hackers from penetrating the security of software-enabled medical devices while simultaneously seeking to provide access to that software to facilitate patient access to stored data and independent security verification.

Similarly, until the rise of the smartphone, the FTC and FCC accepted a congressionally mandated detente over privacy policy in this country. The FTC embraced a role as the preeminent privacy cop, at least over commercial actors, while the FCC focused on its relatively narrow, statutorily provided regulation of Customer Proprietary Network Information ("CPNI").[143] Meanwhile, again by statutory fiat, the FTC ceded authority over the traditional telecommunications in-

---

141 Mike Masnick, *There Are 250,000 Active Patents That Impact Smartphones; Representing One in Six Active Patents Today*, TECH DIRT: INNOVATION, (Oct. 18, 2012, 8:28 AM), https://www.techdirt.com/blog/innovation/articles/20121017/10480520734/there-are-250000-active-patents-that-impact-smartphones-representing-one-six-active-patents-today.shtml [https://perma.cc/UY5M-RBYC].

142 *See supra* notes 66–84 and accompanying text.

143 47 U.S.C. § 222 (2012).

dustry because Congress excluded "common carriers" from its section 5 jurisdiction.[144]

The peace was at least interrupted in 2014's Open Internet Order from the FCC. Through this Order, the FCC reclassified broadband internet service under Title II of the Telecommunications Act.[145] Most importantly for this discussion, this extended the CPNI rules to new actors, treading somewhat into the area the FTC had called its regulatory home.[146] Privacy watchers anticipated a coming turf war, particularly once the FCC began bringing large-dollar judgments against providers for violating the CPNI rules.[147]

We have yet to see how this particular turf war might play out. For now, there appears to be a cease-fire. In late 2015, the FTC and FCC bureau directors in charge of enforcing their respective privacy rules entered into a Memorandum of Understanding, laying out a promise to coexist and cooperate on privacy cases involving providers of communications services.[148]

These examples showcase that varying mandates and policy initiatives will bring regulators to train their sights on computer code in overlapping and sometimes-conflicting ways. Interests in sound cybersecurity policy will run headlong into copyright concerns,[149] interests in patient autonomy into health and safety concerns, and interests in repair and tinkering into environmental and safety concerns.

Moreover, no entity or law currently stands well equipped to evaluate and mediate these policy concerns. While the NTIA's portfolio theoretically involves harmonizing the administration's position on technology-related issues, we believe a more robust set of tools is necessary. While this Article does not provide a complete set of these tools, the next section endeavors to lay a foundation.

C. The Lessons of the CFAA

Whether we embrace a single, omnibus code regulation as a response to the thicket, or continue down our current path of creating

144 15 U.S.C. § 45(a)(2) (2012).

145 In the Matter of Protecting and Promoting the Open Internet, 30 FCC Rcd. 5601, ¶ 133 (2015) (Report and Order on Remand, Declaratory Ruling, and Order).

146 *See id.* ¶¶ 462, 464, 467.

147 Bracy, *supra* note 12.

148 FTC-FCC Consumer Protection Memorandum of Understanding, *supra* note 13.

149 Laura Moy, *Why Copyright Law Is Undermining Cybersecurity, and How to Fix It,* NEW AM. OPEN TECH. INST.: BLOG (June 30, 2015), https://www.newamerica.org/oti/why-copyright-law-is-undermining-cybersecurity-and-how-to-fix-it/ [https://perma.cc/6DAS-TX2J].

new provisions for every context, there is much we can learn from decades-long experience with the CFAA.[150]

Perhaps the most important lesson the CFAA teaches is about the importance of authorization. As earlier scholarship[151] and many of the works in this Symposium[152] demonstrate, those who would regulate code often create elaborate permissions systems, born in software and made enforceable through legislation.[153] When this is done well, these systems draw bright lines that delineate the borders between what is allowed and forbidden.[154] When this is not done well, coders and other actors face uncertainty.[155] This uncertainty is only multiplied in the regulatory thicket, as coders may encounter overlapping or inconsistent expressions of authorization or prohibition.

Professor Ed Felten has experienced the difficulty of doing research on software systems under the "permission" systems created by the CFAA and DMCA, facing challenges from the copyright industry directed at stifling his research.[156] Many innovative researchers require close contact with attorneys in order to steer clear of exposure to liability.[157] Lawyers trying to interpret the ambiguities and open textures of these laws tend to err on the side of caution, providing conservative advice, meaning much research is narrowed or avoided altogether.

What Professor Felten has experienced will begin to trickle outside the rarefied world of computer science research and begin to touch commercial actors and individual tinkerers in fields that to date have been untouched by this kind of fear of regulation. For example, the FAA has required owners of drones that weigh more than about one half of a pound to register and mark their drones[158] and NHTSA

---

150 *E.g.*, Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003).

151 *See id.*

152 *E.g.*, James Grimmelmann, *Consenting to Computer Use*, 84 GEO. WASH. L. REV. 1500 (2016), Josh Goldfoot & Aditya Bamzai, *A Trespass Framework for the Crime of Hacking*, 84 GEO. WASH. L. REV. 1477 (2016).

153 *See id.*

154 *See id.*

155 *See id.*

156 *See* Pam Samuelson, *Anticircumvention Rules: Threat to Science*, 293 SCI. 2028, 2028 (2001).

157 *E.g.*, *id.*

158 Fed. Aviation Admin., *Unmanned Aircraft Systems (UAS) Registration*, FAA, http://www.faa.gov/uas/registration/ [https://perma.cc/H6EW-PDB7] (last modified Sept. 19, 2016, 10:06 AM).

recommends that car manufacturers hire computer security experts to protect their connected cars.[159]

IV. Centralizing Code Regulation

One way to ameliorate some of the problems of turf wars and the looming software regulation thicket is to vest authority for code regulation in a single government agency. There is a modest role for a well-designed and properly-authorized entity to help the federal government speak with one voice and to help anticipate and resolve inconsistencies. To be clear, we do not think it would be wise to centralize all authority for all software regulation. Even once everything has software, there will still be good reason to keep regulatory power divided roughly along historically relevant boundaries.

The most important reason to centralize some authority will be to stamp out, or at least recognize, inconsistencies. Of course, some inconsistencies are not a problem. Agencies might interpret the term "authorization" differently if one is focused on vehicle safety and the other on copyright, for example. But if two agencies purporting to regulate essentially the same thing (for example, the FTC and FCC on privacy) promulgate inconsistent rules or approaches, the results will often be undesirable. In circumstances like these, we might want a centralized agency that can, at the very least, coordinate between the agencies and perhaps serve as adjudicator or tiebreaker, the way the Office of Management and Budget does for executive branch decisions.[160] The prospective agency might also serve as a convening force, bringing together experts from industry, government, the academy, and public interest groups to debate issues, produce research, and educate one another.

For inspiration, we could look to similar efforts along these lines, learning from the roles played in the White House by the Office of Science and Technology Policy and the Office of Management and Budget. We should also consider proposals from scholars, such as a proposal by Frank Pasquale and Oren Bracha to establish a Federal

---

159 Nat'l Highway Traffic Safety Admin., U.S. Dep't Transp., A Summary of Cybersecurity Best Practices 26 (Oct. 2014), http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812075_CybersecurityBestPractices.pdf.

160 *The Mission and Structure of the Office of Management and Budget*, White House, https://www.whitehouse.gov/omb/organization_mission/ [https://perma.cc/RPG8-LFHY] (last visited Oct. 3, 2016).

Search Commission[161] and another from Ryan Calo to establish a Federal Robotics Commission.[162]

The vision thus far is decidedly top-down: one central agency serving as the last word on resolving agency conflicts. We think it is equally important—if not more important—to spur bottom-up expertise at the same time. The top-down regulator can help with this goal too: it can create mandates, incentives, or simply best practice guides, all encouraging agencies to source and incorporate technical experts into their employee ranks.

One model might be the FTC, which has in recent years injected a large and growing number of technologists into the agency, starting first with five successive Chief Technologists, and including the creation of a new Office of Technology Research and Investigation.[163]

A second model is the recently created Federal Privacy Council.[164] This entity, created by White House Executive Order, has been charged with helping "Senior Agency Officials for Privacy at agencies better coordinate and collaborate, educate the Federal workforce, and exchange best practices."[165] The Executive Order also obligated agency heads to designate a "Senior Agency Official for Privacy" (in most cases, a Chief Privacy Officer), if they did not have one already.

We harbor no illusions that the presence of more technical expertise will necessarily solve the thicket problem or avoid agency conflicts. Technical experts might in good faith disagree about a technical problem based on the vantage point of the agency they represent, the information they can access, and the type of training and experience they bring to their positions. Still, we think technical experts at different agencies are likely to agree on core questions about the technology itself. This will isolate for disagreement issues that cannot be resolved based on understanding the technology alone, which we think will both narrow and sharpen the set of important issues in a very productive manner.

---

161 Oren Bracha & Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149, 1151 (2008).

162 Ryan Calo, *The Case for a Federal Robotics Commission*, CTR. TECH. INNOVATION BROOKINGS (Sept. 15, 2014), http://www.brookings.edu/research/reports2/2014/09/case-for-federal-robotics-commission [https://perma.cc/PGR9-JPTZ].

163 Ashkan Soltani, *Booting Up a New Research Office at the FTC*, TECH@FTC BLOG (Mar. 23, 2015, 11:00 AM), https://www.ftc.gov/news-events/blogs/techftc/2015/03/booting-new-research-office-ftc [https://perma.cc/J6N4-T58G].

164 Exec. Order No. 13,719, 81 Fed. Reg. 7959 (Feb. 9, 2016).

165 *Id.* § 4.A.

Conclusion

We used to regulate things, and now we regulate code. As software replaces hardware across every industry and in every sphere of human activity, regulators will realize that they are undertaking what is, for them, at least, a fundamentally new and foreign type of activity. The more insightful and self-aware regulators among them will recognize that they need to change their approaches, philosophies, and personnel to respond to this change. The best regulators will understand that they have lessons to learn from agencies on the vanguard of code regulation, such as the FTC, FCC, and Register of Copyrights, with many of those lessons being cautionary tales rather than best practices. In the end, we think it is likely that the federal government will need to centralize at least some authority over code in a single agency. If we are careful and a bit lucky, we might be able to avoid repeating some of the most difficult mistakes of the CFAA and DMCA.