DIRTY CODE: REGULATORY LESSONS FROM THE VOLKSWAGEN EMISSIONS SCANDAL

EILIF VANDERKOLK*

* Juris Doctor 2018, University of Colorado School of Law and Managing Editor, Colorado Technology Law Journal. This article is dedicated to my late grandfather, Judge Carl Bernard Rubin. I would like to thank Kyriaki Council for her editorial work that made the publication of this article possible, Lindsey Knapton and Parker Ragland for tolerating me in our office this year, and the incredible faculty associated with the Colorado Law technology programs. Specifically, I would like to thank Professor Blake Reid for both his work as our faculty advisor and for introducing me to technology policy advocacy as my clinical professor, and Professor Phil Weiser whose work has been instrumental in establishing CTLJ as a flagship publication in the fields of technology law and policy.

I. THE PROBLEM WITH SOFTWARE IS THE WETWARE

Regulatory and testing regimes are not currently designed to handle software capable of distinguishing between laboratory and real-world conditions. Accordingly, there are strong incentives for a company to subvert compliance testing through software cheats. Unfortunately, the current regulatory testing framework, designed to compel compliance with government standards, is inadequate to catch this subversion. Software is a fundamentally malleable medium, and is much more difficult to assess than the hardware that controlled functions in past generations. Without a better method to analyze the software present in regulated products, consumers are exposed to leaks of their personal information,[1] increased levels of harmful pollutants,[2] and the potential theft of critical intellectual property.[3]

Software applications have become ubiquitously integrated in many products that Americans use in their everyday life. Cellphones, computers, cars, and coffeemakers all use software installed by their manufacturers to provide a better product to their customers. However, ensuring that these devices comply with pertinent regulations is made more difficult when the existing code can be designed to modify a device's behavior when it detects the conditions associated with the testing environments used by regulatory agencies.

Currently, the volume of code written for many commonly used applications is staggering. A million lines of code is approximately 18,000 pages of printed text, which is the equivalent of 14 copies of *War and Peace*, 25 copies of *Ulysses*, or 63 copies of *The Catcher in the Rye*.[4] In contrast, the Android operating system contains 12 million lines of code, Windows 7 used about 40 million lines, and a modern car might have 100 million lines of code in its onboard computers.[5] Since these numbers are only likely to grow in the future, it is important to thoroughly vet code that will run on the devices we depend on.

The opaque nature of complex code has created an incredibly complicated ecosystem of interdependence in software systems. In his book, *Overcomplication*, Samuel Arbesman argued that "[c]omputer hardware and software is much more complex than anything that came before it" and that "[a]s computing has become embedded in everything from our automobiles and our telephones to

1. Jeff J. Roberts, *Creepy Teddy Bears Leak Kids' Voices to Strangers on the Internet*, FORTUNE (Feb. 28, 2017), http://fortune.com/2017/02/28/cloudpets-data-leak/ [https://perma.cc/9JGC-YAL8].

2. Steven R. H. Barrett et al., *Impact of the Volkswagen Emissions Control Defeat Device on US Public Health*, 10 ENVTL. RES. LETTERS, at 5 (2015).

3. Peter Elkind, *Sony Hack*, FORTUNE (June 25, 2015, 6:00 AM), http://fortune.com/sony-hack-part-1/ [https://perma.cc/2SSB-7KRD].

4. DAVID MCCANDLESS, KNOWLEDGE IS BEAUTIFUL (2014).

5. *Id.*

our financial markets, technological complexity has eclipsed our ability to comprehend it."[6] With this complexity in mind, the software industry has developed some techniques to address the problem.

Given that it is exceedingly difficult to physically check every line of code, the software typically uses dynamic testing—which is the examination of the physical response from the system to variables that are not constant and change with time—to conduct validation and verification of written code. [7] These procedures are typically focused on ensuring that the software satisfies specified requirements, and that the products of a given development phase satisfy the conditions imposed at the start of that phase.[8] The tests generally do not look for subtler alterations to the behavior of the code and the device the code is running.

Unfortunately, when a developer is provided with the conditions that their code will be tested under, it is easy to code in behavior that only occurs under these conditions.[9] This fundamentally places testing departments of regulatory agencies in a bind. To be fair, testing conditions should both be disclosed to the tested company, as well as be as consistent between tests as possible. However, when that information is available it can be used to subvert the intent of the test. This is what occurred in the Volkswagen diesel emissions scandal, and a study of this event will hopefully shed light on how regulation and enforcement can occur in an increasingly complex environment.[10]

This Article will use the Volkswagen diesel emissions violation as a case study to demonstrate how manufacturers can easily circumvent regulatory testing through software. After understanding exactly what Volkswagen did, this Article will examine alternative regulatory models that are used outside of the Environmental Protection Agency (EPA). These regulatory models will cover the Federal Communications Commission (FCC) as an example of government regulation, software testing used in the private sector, and the public/private model employed by Underwriters Laboratory (UL). Finally, this Article will propose a joint body run by private industry, and encouraged by the federal government, to certify to consumers and regulatory agencies that no malicious code is present.

6. SAMUEL ARBESMAN, OVERCOMPLICATED: TECHNOLOGY AT THE LIMITS OF COMPREHENSION 3 (2016).

7. GLENFORD J. MYERS ET AL., THE ART OF SOFTWARE TESTING (3rd ed. 2011).

8. IEEE STANDARDS BOARD, IEEE STANDARD GLOSSARY OF SOFTWARE ENGINEERING TERMINOLOGY 85 (2002).

9. Arnold W. Reitze Jr., *The Volkswagen Air Pollution Emissions Litigation*, 46 ENVTL. L. REP. NEWS & ANALYSIS 10564 (2016).

10. *Id.*

II. VOLKSWAGEN'S DIRTY SECRETS

A. Better Living Through Clean Diesel

In 2015, the EPA announced that 482,000 Volkswagen diesel engine vehicles sold in the United States were programmed to pass emissions tests, but when operating under normal driving conditions, emit air pollutants well above the legal limit.[11] This violation was discovered by West Virginia University's (WVU) Center for Alternative Fuels, Engines, and Emissions (CAFEE).[12] CAFEE discovered the violation while conducting testing to determine how Volkswagen was meeting U.S. emission standards that were more stringent than Europe's, and was referred to the EPA and California regulators.[13]

The EPA and California regulators investigated, and Volkswagen admitted that it deliberately outfitted its cars with defeat devices.[14] A defeat device is a piece of hardware or software installed in a vehicle that will allow the vehicle to pass EPA testing when the emissions would otherwise fail to pass EPA standards. Per the EPA, Volkswagen inserted lines in the computer code governing the engine performance that activates the emissions controls when driving patterns are detected that are consistent with the testing protocol.[15] When the vehicle's operation is consistent with road use, the engine maximizes fuel economy, but emissions increase dramatically.[16]

What CAFEE uncovered was that a piece of code in the computer controlling the vehicle's engine could detect testing conditions. Per the EPA, when the car detected a test from steering patterns, barometric pressure, or only two wheels spinning, it would engage a mode called dyno calibration, which made the car emit less nitrous oxide (NO_x), but sacrificed fuel efficiency and engine power.[17]

This fraudulent workaround was likely introduced by Volkswagen to deal with the particular combination of emissions regulation and technology present in 2007.[18] In 2007, Volkswagen decided not to use the Daimler BlueTEC technology, due to the drawbacks inherent in the system.[19] Volkswagen wanted to avoid the use of urea tanks, which are expensive, take up space, are an incon-

11. *Id.*
12. *Id.*
13. Dune Lawrence et al., *How Could Volkswagen's Top Engineers Not Have Known?*, BLOOMBERG BUSINESSWEEK, Oct. 26, 2015, at 52.
14. *Id.*
15. *Id.*
16. *Id.*
17. *Id.*
18. *Id.*
19. Daimler BlueTEC sprays urea into the exhaust stream to neutralize NOx formation, but requires an additional chemical tank built into the vehicle.

venience to consumers, and required compliance with EPA regulations that were difficult or impossible to meet.[20]

Instead, Volkswagen went with Lean NO, a system that injects extra fuel into the engine and the exhaust system.[21] This requires accurate calibration of the onboard engine control computer to deal with the tradeoff between increased NO_x emissions as combustion temperature increases and the improved fuel economy that higher temperature combustion provides.[22] Unfortunately, it appears that the system could not meet the stringent EPA NO_x emission standards while preserving the fuel economy advantages of diesel technology.[23]

While the Volkswagen defeat device allowed them to bring diesel cars to market in the U.S., it is estimated that the cost of this emission cheating will be approximately $18.2 billion.[24] The Department of Justice (DOJ) has also filed a civil complaint against Volkswagen, Audi, and Porsche for violations involving defeat devices in about 500,000 two-liter diesel engine vehicles and about 85,000 three-liter diesel engines.[25] The DOJ is also conducting a criminal investigation against these companies, as the Clean Air Act's §113(c)(2) provides for criminal fines and imprisonment for up to two years for false statements and certifications, which includes any person who knowingly "falsifies, tampers with, renders inaccurate, or fails to install any monitoring device or method required to be maintained or followed under this chapter."[26]

B. Predictable Testing

Many of the non-compliance problems that the EPA has faced are attributable to the predictable way the EPA tests vehicles. This predictability allows companies like Volkswagen to tailor the operation of their vehicles to behave differently under specific testing conditions, which the EPA clearly lays out.

The National Vehicle and Fuel Emissions Laboratory (NVFEL) in Ann Arbor, Michigan utilizes specialized equipment to accurately measure emissions from a wide range of vehicles and engines.[27] This laboratory has several responsibilities, including testing new and

20. Dune Lawrence et al., *West Virginia University Research Group Revealed VW Engineers' Emissions Cheating*, 46 DAILY ENV'T REP. (BNA) 3219, 3221 (Oct. 23, 2015).

21. *Id.*

22. *Id.*

23. *Id.*

24. Patrick Ambrosio, *Volkswagen More Than Doubles Estimate on Total Cost of Diesel Emissions Scandal*, 47 DAILY ENV'T REP. (BNA) 1295 (Apr. 29, 2016).

25. Press Release, DOJ, United States Files Complaint Against Volkswagen, Audi and Porsche for Alleged Clean Air Act Violations (Jan. 4, 2016), https://www.justice.gov/opa/pr/united-states-files-complaint-against-volkswagen-audi-and-porsche-alleged-clean-air-act [https://perma.cc/4VJG-WH48].

26. Clean Air Act §113, 42 U.S.C. §7413(c)(2)(C) (2012).

27. *Vehicle and Engine Emissions Testing*, EPA, https://www.epa.gov/vehicle-and-fuel-emissions-testing/vehicle-and-engine-emissions-testing-national-vehicle-and-fuel [https://perma.cc/GM7Z-3PYL] (last updated Jan. 23, 2017).

used cars, light trucks, and heavy-duty vehicles to ensure they meet emissions standards when they are new and throughout their useful lifetime; researching and testing to inform new and updated emissions standards for air pollutants; developing and implementing accurate test methods for measuring emissions from vehicles and engines; and assessing promising emissions-reduction technologies.[28]

At this lab, cars and light trucks are tested on a chassis dynamometer, which consists of one or two large rollers connected to an electric motor, under tightly-controlled conditions that simulate the operation of a vehicle on the road. To evaluate exhaust emissions and fuel economy performance in a way that is accurate and repeatable, vehicles are driven on a dynamometer over standard test cycles. These tests involve a dynamometer; the vehicle being tested driven on the rollers, which simulate the speed and resistance of an actual road; and sophisticated chemical analyzers which measure pollutants from the vehicle exhaust.[29]

C. Regulation and Post-Hoc Enforcement

Prospective regulation and post-hoc enforcement can both be used to constrain the behavior of a regulated industry. However, over reliance on enforcement to corral illegal behavior can result in companies making calculated gambles regarding the likelihood of exposure and the potential gain of violating a rule. This is particularly concerning when dealing with the potential harms to consumers and the environment, such as higher death rates and increased levels of greenhouse gasses, that cannot be easily resolved through fines and compensation.

This is not the first time that vehicle manufacturers have tried to defeat auto-emissions testing. The EPA has had to deal with this issue several times in the last several decades, and has had settlements with major manufacturers over defeat devices installed in their cars.[30] These violations have occurred despite specific prohibitions against defeat devices in automobiles that already exist. These prohibitions state:

> (a) No new heavy-duty vehicle or heavy-duty engine shall be equipped with a defeat device.
>
> (b) The Administrator may test or require testing on any vehicle or engine at a designated location, using driving cycles and conditions which may reasonably be expected to be encoun-

28. *Id.*
29. *Id.*
30. *GM to Recall 470,000 Cadillacs, Pay Fine Over Charge That Device Raised Emissions*, DAILY ENV'T REP. (BNA), at AA-1 (Dec. 1, 1995); Statement of Carol M. Browner, Adm'r, EPA, DOJ/EPA Press Conference, Settlement of General Motors Enforcement Action (Nov. 20, 1995) (transcript available at 1995 WL 705249).

> tered in normal operation and use, for the purpose of investigating a potential defeat device.
>
> (c) [Reserved]
>
> (d) For vehicle and engine designs designated by the Administrator to be investigated for possible defeat devices:
>
> (1) General. The manufacturer must show to the satisfaction of the Administrator that the vehicle or engine design does not incorporate strategies that reduce emission control effectiveness exhibited during the applicable Federal emissions test procedures when the vehicle or engine is operated under conditions which may reasonably be expected to be encountered in normal operation and use, unless one of the specific exceptions set forth in the definition of "defeat device" in § 86.004–2 has been met.
>
> (2) Information submissions required. The manufacturer will provide an explanation containing detailed information (including information which the Administrator may request to be submitted) regarding test programs, engineering evaluations, design specifications, calibrations, on-board computer algorithms, and design strategies incorporated for operation both during and outside of the applicable Federal emission test procedure.[31]

In 1995, the EPA and the DOJ announced a settlement with General Motors (GM) for alleged violations of the Clean Air Act. GM paid approximately $45 million to settle federal government charges that it installed illegal devices that defeat pollution controls inside nearly a half-million Cadillacs, and agreed to recall and fix more than 470,000 late-model Cadillacs.[32] GM spent approximately $30 million recalling the cars to eliminate the defeat device that caused the excess emissions.[33]

In 1998, the EPA settled a variety of defeat device cases. First, the EPA resolved charges that the companies Caterpillar Inc., Cummins Engine Company, Detroit Diesel Corporation, Mack Trucks, Inc., Navistar International Transportation Corporation, Renault Vehicules Industriels, s.a., and Volvo Truck Corporation violated the Clean Air Act by installing devices that defeat emission controls.[34] Secondly, Honda was alleged to have used emissions defeat devices, paid a

31. 40 C.F.R. § 86.004–16.
32. EPA, *supra* note 27.
33. *Id*.
34. Press Release, EPA, DOJ, EPA Announce One Billion Dollar Settlement with Diesel Engine Industry for Clean Air Violations (Oct. 22, 1998), https://archive.epa.gov/ [https://perma.cc/DE8P-SXBY] (search "diesel engine industry"; then follow "10/22/98" hyperlink).

civil penalty of $12.6 million, and incurred remedial costs of $250 million.[35] Also in 1998, Ford Motor Co. faced similar allegations, paid a civil penalty of $2.2 million, and incurred remedial costs estimated at $7.5 million.[36]

Finally, in 2005, Volkswagen paid $1.1 million to resolve its failure to promptly notify the EPA of defective oxygen sensors and for failing to correct the same defective sensor, which affected at least 329,000 of their 1999, 2000, and 2001 Golfs, Jettas, and New Beetles.[37]

Despite a lengthy history of expensive financial settlements, vehicle manufacturers have still found it profitable to engage in fraudulent behavior when passing their vehicles through the EPA's emissions testing. It seems apparent that the current model of regulation and enforcement has not sufficiently prevented this behavior.

Post hoc enforcement can allow significant harm to occur before the violation is caught, and continuing to use *post hoc* enforcement to prevent illegal software modifications will be a particularly costly model in the realm of environmental regulations. It is estimated that approximately fifty-nine early deaths will eventually be caused by the 2008–2015 excess emissions, with a monetized cost of approximately $450 million, and that there will be approximately thirty-one cases of chronic bronchitis, approximately thirty-four hospital admissions, approximately 120,000 minor restricted activity days, approximately 210,000 lower respiratory symptom days, and approximately 33,000 days of increased bronchodilator usage.[38] Per kilometer driven, this mortality rate from excess NO_x is approximately twenty percent of the accident fatality rate for an average U.S. passenger car.[39]

In fact, it appears that other vehicle manufacturers have not been discouraged from following a path similar to Volkswagen's. On January 12, 2017, the EPA "issued a notice of violation to Fiat Chrysler Automobiles N.V. and FCA US LLC (collectively FCA) for alleged violations of the Clean Air Act for installing and failing to disclose engine management software in certain light-duty diesel vehicles sold in the United States."[40] While Fiat Chrysler has denied these allegations and asserted that the software merely exists as part of an overall strategy to "reduce tailpipe emissions without compromising the durability and performance of its engines," the issue remains un-

35. Reitze, *supra* note 9.

36. *Id.*

37. Press Release, EPA, Volkswagen of American, Inc., Agrees to Pay More Than $1 Million for Clean Air Act Violation, (June 15, 2005), https://yosemite.epa.gov/opa/admpress.nsf/blab9f485b098972852562e7004dc686/6946eeaadcfa982b8525702100777c0e [https://perma.cc/F9UR-GQJL].

38. Steven R. H. Barrett et al., *Impact of the Volkswagen emissions control defeat device on US public health*, 10 ENV'T RES. LETTERS 5, 6–7 (2015).

39. *Id.*

40. *FCA (Fiat Chrysler Automobiles) Diesel Vehicle Violations*, EPA, https://www.epa.gov/fca/learn-about-fca-violations [https://perma.cc/2F37-V7TB] (last visited Nov. 2, 2017).

der an EPA enforcement action.[41] Given that this behavior seems unlikely to be stopped through existing regulatory strategies, it would be appropriate for regulatory bodies to begin examining alternative methods of software verification.

III. ALTERNATIVE REGULATORY COMPLIANCE MODELS

Compliance testing undertaken by a single laboratory is not the only way that products can be verified to comport with federal statutes, regulations, and standards. For example, the FCC authorizes several other independent bodies to certify equipment, while private industry has developed their own software assurance techniques.[42] Additionally, Underwriters Laboratories (UL) exists as a private group that is nationally recognized in fire prevention certification.[43]

A. FCC Authorization Model

The FCC employs a different model than the EPA of ensuring regulatory compliance on devices it certifies. Rather than conducting testing in-house, the FCC authorizes certain organizations to test equipment for it.[44] These groups are known as Telecommunication Certification Bodies (TCB) and they have the authority to issue Certifications for compliance with FCC regulations.[45] Utilizing TCBs, the FCC recognizes three different levels of authorization: certification, declaration of conformity, and verification.[46] These three levels allow the FCC to determine what is an appropriate level of stringency based on the potential harm of a device.[47]

The highest level of review that the FCC requires for the most potentially hazardous devices is Certification, and this is the most rigorous approval process for Radio Frequency Devices.[48] Certification is an equipment authorization handled by a recognized TCB based on an application and testing data submitted by the manufacturer or importer.[49] The TCB then examines the test data and supporting documentation to determine whether the testing followed appro-

41. Steven Overly & Brady Dennis, *EPA: Fiat Chrysler software enabled emissions cheating*, WASH. POST (Jan. 12, 2017), https://www.washingtonpost.com/news/innovations/wp/2017/01/12/epa-fiat-chrysler-used-software-to-cheat-on-emissions-tests/ [https://perma.cc/B7D8-Y5MN].

42. 47 C.F.R. § 2.901 (2013).

43. UNDERWRITERS LAB., http://www.ul.com/ [https://perma.cc/8QN3-BP87] (last visited Nov. 2, 2017).

44. *Equipment Authorization*, FCC, https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization [https://perma.cc/3RQZ-FY6X] (last visited Mar. 24, 2017).

45. *About TCBC*, TCB COUNCIL, http://www.tcbcouncil.org/?page=A1 [https://perma.cc/HL3U-WUA3] (last visited Mar. 24, 2017).

46. *See* FCC, *supra* note 44.

47. 47 C.F.R. § 2.902 (2017); 47 C.F.R. §§ 2.906–2.907 (2017).

48. *See* FCC, *supra* note 44.

49. *Id.*

priate protocols and the data demonstrates technical and operational compliance with all pertinent rules.[50]

At the next level, a Declaration of Conformity (DoC) requires the party responsible for compliance to use an accredited testing laboratory that follows established measurement protocols to ensure that the equipment complies with the appropriate technical standards.[51] The responsible party is not required to file an equipment authorization application with the FCC or a TCB, as it would for a certification, and equipment authorized under the DoC procedure is not listed in any FCC database.[52] However, the responsible party must provide a test report and other information demonstrating compliance with the rules upon request by the Commission.[53]

Finally, verification requires the least amount of compliance work.[54] Verification requires that the party responsible for compliance rely on measurements that it, or another party, makes on its behalf, to ensure that the equipment complies with the appropriate technical standards.[55] The responsible party is not required to use an accredited testing laboratory, it is not required to file an application with a TCB, and equipment authorized under the verification procedure is not listed in any Commission database.[56] However, the responsible party must provide a test report and other information demonstrating compliance with the rules upon request by the Commission.[57]

This model of employing outside facilities to ensure compliance would allow a wider array of tests to occur on regulated devices and, in many ways, is similar to the method that initially uncovered the Volkswagen fraud. The independent research undertaken by WVU, at the behest of the International Council on Clean Transportation, only uncovered the discrepancy between lab conditions and real-world driving when the cars were removed from the dynamometers and taken on road tests.[58] The tiered compliance model also allows lower compliance costs for devices that are less likely to be harmful and need less rigorous testing to demonstrate this to the Commission.

However, this model does have its own drawbacks. Introducing a variety of labs to the existing testing procedures would introduce more variability into the existing test framework. Even if procedures were standardized across labs, it would be easy to see how small discrepancies might work themselves into tests and create an environment where regulated entities seek out the most lenient of these

50. *Id*.
51. *Id*.
52. *Id*.
53. *Id*.
54. 47 C.F.R. § 2.902.
55. FCC, *supra* note 44.
56. *Id*.
57. *Id*.
58. Lawrence, *supra* note 13, at 52.

facilities. Additionally, labs that are tightly controlled by a regulatory agency are probably not going to be flexible enough to keep up with the changes in software and security.

B. Software Assurance Model

Enhanced testing designed to catch defeat devices is likely to result in an arms race between regulators and bad actors seeking to circumvent the tests. As an alternative to this type of testing, agencies could adopt a cross-agency software assurance framework similar in scope to the Federal Information Security Management Act (FISMA).[59] The FISMA was U.S. legislation that defined a comprehensive framework to protect government information, operations, and assets against natural or man-made threats.[60]

This approach would include techniques like black box testing. With black box testing, the software tester does not have access to the source code itself. The code is a "big black box" to the tester who cannot see inside the box. The tester knows only that information can be input into to the black box, and the black box will send something back out. Based on the requirements knowledge, the tester knows what to expect the black box to send out and tests to make sure the black box sends out what it is supposed to send out.[61]

FISMA assigns responsibilities to various agencies to ensure the security of data in the federal government. The Act requires program officials, and the head of each agency, to conduct annual reviews of information security programs, with the intent of keeping risks at or below specified acceptable levels in a cost-effective, timely, and efficient manner. This Act lays out a framework for all federal agencies to follow when they enact security management plans, and tasks the National Institute of Standards and Technology (NIST) with supporting these efforts.[62]

To aid in compliance with the FISMA, NIST has outlined several general guidelines, such as:

- Categorizing the information to be protected;
- Selecting minimum baseline controls;
- Refining controls using a risk assessment procedure;
- Documenting the controls in the system security plan;
- Implementing security controls in appropriate information systems;
- Assessing the effectiveness of the security controls once they have been implemented;

59. 44 U.S.C. § 3541 (2012).

60. Federal Information Security Management Act, 40 U.S.C. § 11331 (2012).

61. Laurie Williams, *Testing Overview and Black-Box Testing Techniques*, REALSEARCH (2006), http://www.cs.unc.edu/~hedlund/programming/testing/LaurieWilliams/BlackBox2.pdf [https://perma.cc/PLG6-9MP2].

62. 44 U.S.C. § 3541 (2012).

- Determining agency-level risk to the mission or business case;
- Authorizing the information system for processing; and
- Monitoring the security controls on a continuous basis[63]

Under this framework, NIST has also established a wide array of whitepapers and best practices for agencies to follow when assuring the software and applications that run on their own devices. For example, NIST released a special publication "Vetting the Security of Mobile Applications" designed to help secure mobile devices and the applications which run on them.[64] Here, NIST recommended "organizations should develop security requirements that specify, for example, how data used by an app should be secured, the environment in which an app will be deployed, and the acceptable level of risk for an app."[65]

Application vetting as described by NIST is comprised of two main activities: testing and approval/rejection. Testing activity involves the testing of an app for software vulnerabilities by services, tools, and humans to derive vulnerability reports and risk assessments, while app approval/rejection activity involves the evaluation of these reports and risk assessments, along with additional criteria, to determine the app's conformance with organizational security requirements and, ultimately, the approval or rejection of the app for deployment on the organization's mobile devices.[66]

Black box testing would be useful here, because it is a method of software testing that examines the functionality of an application without peering into its internal structures or workings.[67] Specific knowledge of the application's code/internal structure and programming knowledge in general is not required, and test cases are built around specifications and requirements, i.e., what the application is supposed to do.[68]

Additionally, agencies would have to be able to verify and validate the software they are testing. Verification is the process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase, while validation is the process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.[69]

63. Federal Information Security Management Act, *supra* note 60.

64. Steve Quirolgico et. al, *Vetting the Security of Mobile Applications*, NAT'L INST. OF STANDARDS & TECH. (Jan. 2015), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf [https://perma.cc/A2YN-NUYM].

65. *Id.*

66. *Id.*

67. Laurie Williams, *supra* note 61.

68. *Id.*

69. *Id.*

However, this would impose additional costs on compliance testing. While software testing is focused on efficiently determining problems with code, it is estimated that testing and verification activities can range from 50 to 75 percent of the total development costs.[70] It might also introduce the same sort of variance between tests that we sought to avoid with the independent lab method.

Unfortunately, the nature of the software world makes the application of governmental standards difficult. Agencies face much larger bureaucratic hurdles and have difficulty keeping up with the pace of much slower industries than software development.[71] Given these constraints, it is likely that placing most of the burden on the federal government to regulate software imported and sold within the U.S. would result in a bureaucracy that would struggle with keeping abreast of the most recent developments and would harm technical innovation in a critical field.

C. Underwriters Laboratory

There are alternative models under which software can be verified, and there is still a role for government participation in this process. In this scheme, government would act as a facilitator and intermediary for industry partners in the development of an independent lab built in the model of the existing UL.

1. UL Framework

UL was started in 1894 to test the safety of proposed electrical products and ensure that they would not pose a significant fire risk.[72] In 1899, their testing included arc lamps, bushings, circuit breakers, cleats, conduits, fire alarm boxes, flexible cords, fuses, heaters, fixture installation joins, junction boxes, lamp adjusters, and rheostats.[73] As technology advanced, so did the products that UL tested. Now, UL focuses on "the next generation of safety challenges, helping new geographies, new industries and new stakeholders create safer living and work environments."[74] These include emerging electrical technologies in electric cars, solar cells, and wind turbines.[75]

UL has a wide-ranging mission, focused primarily on electrical safety: "UL certifies, validates, tests, verifies, inspects, audits, advises and educates;"[76] they "provide the knowledge and expertise to help

70. B. Hailpern & P. Santhanam, *Software debugging, testing and verification*, 41 IBM SYSTEMS J. 4 (2002).

71. Reitze, *supra* note 9.

72. *See History*, UL, http://www.ul.com/aboutul/history/ [https://perma.cc/2S78-C8R6] (last visited Nov. 2, 2017).

73. *Id.*

74. *Id.*

75. *Id.*

76. *What We Do*, UL, https://www.ul.com/aboutul/what-we-do/ [https://perma.cc/U2BY-GLB2] (last visited Nov. 2, 2017).

customers navigate growing complexities across the supply chain from compliance and regulatory issues to trade challenges and market access;"[77] and "facilitate global trade and deliver peace of mind."[78] These governing principals could easily be applied to an independent body designed to certify software as secure and designed to carry out the software's intended goals without malicious behavior hidden in the executable programming.

Essentially, UL offers an independent certification on new products to assure both consumers and corporate partners that products certified by them will meet the applicable standards. For example, when searching for components to be integrated into a laptop charger, the assembling company has to know that each part they purchase will not pose some unknown risk to the final product. Additionally, the completed device is then also often certified under UL's standards.

2. IP Protections

For this type of collaborative model to be successful, companies would have to turn over complete copies of their intended software, which are likely to contain large amounts of proprietary code and other intellectual property. Once the code leaves their hands, it is hard to know that it remains securely in the possession of the standards organization, as a copy of code is easy to make, unlike physical products that someone might notice were missing.[79] While the financial impact of a leak will vary between the type of final product, every company is likely to have at least some proprietary code in their systems.[80]

a. Patent Protections

The closest comparison to this process that exists in the current U.S. regulatory framework is the Food and Drug Administration's (FDA) new drug application approval. Under this process, manufacturers submit investigational new drug applications that include sufficient preclinical data to justify the testing of drugs on humans.[81] Patents on these new drugs are often secured before the completion of the human trials, as the Patent and Trade Office has a lower stand-

77. *Id*.
78. *Id*.
79. Aseem Kishore, *Best Tools for Copying a Large Number of Files in Windows*, ONLINE TECH TIPS (Mar. 20, 2014) http://www.online-tech-tips.com/software-reviews/tools-for-copying-many-files/ [https://perma.cc/29DE-98JA].
80. Ben Kepes, *Open Source Is Good And All, But Proprietary is Still Winning*, FORBES (Oct. 2, 2013, 2:41 PM), https://www.forbes.com/sites/benkepes/2013/10/02/open-source-is-good-and-all-but-proprietary-is-still-winning/#71ef972f637a [https://perma.cc/TMR9-54AV].
81. WORLD INTELL. PROP. ORG., INTELLECTUAL PROPERTY HANDBOOK ch. 10, at 9 (2nd ed. 2008) [hereinafter IP HANDBOOK].

ard than the FDA, and so the information is afforded the usual protections of the U.S. patent system.[82] However, companies in this space must protect their product, as "even if another company does not patent the product, the innovating company must be careful not to disclose the invention, otherwise the innovating company would have one year to file the patent before the patent enters the public domain."[83]

While the FDA process is somewhat equivalent to the type of screening process that would be implemented, it would need to be drastically shortened to have a useful impact on software assurance. The FDA approval process "usually requires 10 to 12 years and $100 to $500 million."[84] Any certification process that approaches this length or expense is likely to render the certification impractical for an industry that changes as rapidly as software development. Additionally, the patent application process is also of limited utility here, as the process currently takes about two years to finish.[85]

b. Confidential Information

The other issue to consider here is the difference between the protections offered to data generated for regulatory needs and confidential information. When companies or institutions spend time and money to demonstrate that a product is safe and efficacious, the investment is protected by securing the data generated through this effort.[86] This protection is crucial in highly regulated fields where product safety and efficacy are critical. The importance of protecting such data is recognized in the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Article 39.3.[87] The need for such protection has arisen as the testing necessary to secure regulatory approvals has become more extensive and expensive.[88] Thus, greater incentives for undertaking such work are needed, especially since no other forms of protection may be available for a product that regulatory agencies have authorized for the market.

The protection of data generated for regulatory purposes prevents use of the data by subsequent applicants seeking marketing authorization for the same product. The protection applies unless the subsequent applicant has obtained the consent of the party that first filed the data and obtained the original marketing authorization.[89] It

82. *Id*.
83. *Id*.
84. *Id*.
85. *Patents Data at a Glance*, USPTO, https://www.uspto.gov/dashboards/patents/main.dashxml [https://perma.cc/623J-6UM7] (last visited Nov. 2, 2017).
86. IP HANDBOOK, *supra* note 81.
87. Agreement on Trade-Related Aspects Of Intellectual Property Rights art. 41, Apr. 15, 1994, 1867 U.N.T.S. 154.
88. IP HANDBOOK, *supra* note 81.
89. *Id*.

is often uneconomic for subsequent applicants to generate their own data independently, so this exclusivity effectively confers a *de facto* right in favor of the first applicant.[90] However, the protection is for a limited time, so that subsequent applicants can use it after an appropriate period. This avoids the need for repetitive testing, which is desirable from an economic point of view.[91]

While this point primarily applies to testing that must be done of humans or animals, and therefore carries a stronger moral imperative to avoid unnecessary duplication, it can also be applied to software testing. Certain portions of software included in consumer goods should remain confidential and protected from public exposure that would be detrimental to the informational rights of the company that produced it. However, consumers and competitors should have some access to data to reduce duplicative effort and increase software transparency.

This distinct protection needs to be provided due to the differences between the information necessary for a patent and the data needed for effective regulation, as "proving safety and efficacy for regulatory authorities is a very different matter from demonstrating that an invention is patentable."[92] However, there are additional concerns with moving the regulation of software entirely into a private organization.

Once private companies enact standards that are adopted as law by a regulatory body an additional regulatory cost is imposed on all market participants. Peter Strauss describes this problem eloquently in his recent article.[93]

> If standards have been made into law, don't they have to be public? Don't American citizens and companies have a right to read laws governing their conduct without having to pay the monopoly price a valid copyright would permit a private organization "owning" that legal obligation to charge for permitting access to it, on such terms as it chose to require? As the U.S. Copyright Office well knows, law is not subject to copyright. The Information Age now makes it trivial to provide access that may have been more difficult in the age of print, and federal agencies in particular have for almost two decades been under a statutory duty to make all regulations and other matter affecting private conduct available in the electronic reading rooms they are obliged to maintain. All materials

90. *Id*.
91. IP HANDBOOK, *supra* note 81, at 10.
92. *Id*.
93. Peter L. Strauss, *Private Standards Organizations and Public Law*, 22 WM. & MARY BILL RTS. J. 497, 507 (2013).

placed there are freely available to anyone with access to the Internet.[94]

Private standards that actually, or effectively, become codified into law can create a barrier to innovation because they impose an additional cost on the parties that must comply with them. While these costs would not exist in the same form under a federally run software assurance program, they could be imposed by the operation of private standards agencies. For example, UL sells just one of its three volumes on cybersecurity assurance for several hundred dollars.[95] While this is not an enormous cost, it could stifle small tech startups and the sort of garage programmer who currently operates with very little oversight.

3. IP Sharing

The establishment of this kind of certification organization could also lead to greater sharing of software between participants, as more standardized software would be easier to certify. While not the primary focus of this paper, there are several models for collaborative use of intellectual property that can be used.[96] These include patent pools, patent commons, license of rights, non-assertion pledges, preferential licensing, public domain, and open source.

Patent pools and patent commons both involve a common group of participants who agree to license their technology to each other, or to refrain from requiring royalty payment from other group participants.[97] This model works well for companies who operate in similar fields, and would each benefit from the patents of the other participants. However, entry into a group is difficult without a comparable patent portfolio that would provide value to the other participants.

Alternatively, license of right or non-assertion pledges allow a single patent holder to enable a large group of companies to use their intellectual property without being in a fixed group.[98] By either requiring a licensing agreement, or by making their technology widely available by legally pledging not to assert their patent rights against anyone using the technology, intellectual property shared under this model makes new intellectual property available to new market entrants.

---

94. *Id*.

95. UL STANDARDS SALE SITE, http://www.shopulstandards.com/ProductDetail.aspx?productId=UL2900-1_1_B_20170705(ULStandards2) [https://perma.cc/WJL4-T6LD] (last visited Oct. 16, 2017).

96. Antony Taubman, *Sharing technology to meet a common challenge*, WIPO MAGAZINE (Mar. 2009), http://www.wipo.int/wipo_magazine/en/2009/02/article_0002.html [https://perma.cc/52Z7-9A27].

97. *Id*.

98. *Id*.

Finally, public domain or open source distribution totally removes the patent protections from the intellectual property. Often, technologies are patented in a relatively small number of countries, effectively placing them in the public domain in all other countries as soon as the patent applications are published. Here, these models would permit others to use and adapt the intellectual property, and to redistribute it, regardless of whether it is modified.[99]

4. Government Involvement

The US government has followed this type of model for other important parts of the U.S. economy. For example, the Department of Homeland Security has established a program to encourage supply chain security. Their strategy establishes "[a] government-wide vision of our goals, approach, and priorities to strengthen the global supply chain system."[100] First, this strategy aims to promote "the efficient and secure movement of legitimate goods and fostering a global supply chain system that is resilient to natural as well as manmade disruptions."[101] Additionally, it seeks to establish "the approach the United States Government will rely upon to achieve these goals – namely risk management and coordinated engagement with key stakeholders who also have key supply chain roles and responsibilities."[102] In particular, the strategy focuses on the worldwide infrastructure by which goods are moved from the point of manufacture to the end consumer.[103]

The relevant focus here for this paper is the reliance on the engagement of key stakeholders. The U.S. can provide the information and intelligence that they possess, which might otherwise be unavailable to private companies. This can facilitate better management of that company's supply chain and better protection to the that rely on the timely deliverance of verified products.

This enables the participant stakeholders to combine the flexibility of the private sector with the advantages of the non-competitive nature of government interest. Companies are not competing in the field in information gathering, and are instead operating with the highest level of knowledge available to make informed decisions. It also allows the federal government to act as a negotiator if a dispute should arise between companies and for them to act as an encouraging force for the participating companies to remain in compliance with the guidelines created in the strategy.

99. *Id*.
100. DEP'T OF HOMELAND SEC., NATIONAL STRATEGY FOR GLOBAL SUPPLY CHAIN SECURITY IMPLEMENTATION (2012).
101. *Id*.
102. *Id*.
103. *Id*.

Additionally, it allows the U.S. to create specific priorities to focus on as new issues emerge. For example, in 2013, the DHS decided it would focus on assessing the "cyber security related risks to DHS systems used to collect, maintain, and analyze commercial data as well as systems operated on behalf of DHS necessary to secure the exchange of this data among private and public stakeholders."[104] Allowing priorities to be decided by an agency driven by considerations other than quarterly profit reports can create a more forward looking environment for the standards.

IV. A GUIDING STAR

My proposed solution to the issue of software assurance for commercial and consumer software products would encompass some of the existing government regulatory tools and combine in a joint public-private certification body capable of issuing guidance and ratings for software. Much in the same way that the Energy Star program has been designed to "reduce energy consumption, improve energy security, and reduce pollution through voluntary labeling of or other forms of communication about products," a similar effort could work for better software assurance.[105]

A. Membership

Much like the Energy Star model, membership in this certification body should be completely voluntary. Energy Star has accumulated over 16,000 partners across a wide array of sectors through voluntary labeling and the power of their brand.[106] However, this has required significant investment in the promotion of their brand, and would require a sustained initiative to persuade consumers as to the value of software assurance and data security.

Energy Star had the organizational power of the EPA to initially get it off the ground, and it could potentially require a similar initial effort to create the organization proposed here. Unfortunately, the U.S. has not currently assigned cybersecurity wholly to a single government agency, and as a result it would likely be a much more complicated endeavor to launch a new certification organization.

B. Rating System

This rating would function much like the pass-fail system employed by Energy Star, but intended to certify that the software contains no malicious or hidden functions, and is reasonably secure. Commercial buyers of components for their own products would be

104. *Id.*
105. 42 U.S.C. § 6294(a) (2012).
106. *About Energy Star*, ENERGY STAR, https://www.energystar.gov/about [https://perma.cc/6NYY-UH5A] (last visited Nov. 2, 2017).

able to rely on this verification to ensure that there will not be major data leaks to bad actors simply because of who programmed their widgets.

Vulnerabilities in telecommunications components are likely to be the strongest hook to get major commercial operators to back this type of verification. For instance, companies such as AT&T and Verizon have a commercial interest in ensuring that their proprietary information is protected, as well as a national security obligation to ensure that the communications infrastructure of the U.S. is not penetrated by foreign adversaries simply because they could undercut their competitors thanks to financial support from those same foreign entities.[107]

Additionally, government customers would be able to have the software of regulated devices verified by an expert and neutral third party without having to develop that expertise independently within each agency or in an entirely new governmental body. As the Volkswagen case study has shown, even though software defeat devices have been utilized in the past, the EPA did not attempt to verify the behavior of the software that would control the emissions of the car.

Other regulatory approval bodies are likely to face similar challenges in the future. For example, as artificial limbs and organs become a common part of medicine, the FDA must be able to verify that the software of the device conforms to their expectations once it leaves controlled tests.[108] Additionally, the FCC needs to be able to ensure that transmitters do not alter their behavior with a software defined radio that moves the transmission outside of permitted bands.

C. Governmental Influence

Government actors would likely exert two types of influence over the verification organization. First, they would be able to act as a neutral mediator for any conflicts that might arise between the various interest groups during the creation and operation of the verification process, and government contracts could begin to require the verification to encourage participation by software developers. In fact, a piece of legislation has been proposed by U.S. Sens. Mark R. Warner (D-VA) and Cory Gardner (R-CO), co-chairs of the Senate

107. *Communications Sector*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/communications-sector [https://perma.cc/2AYM-NGK6] (last visited Nov. 2, 2017).

108. *Artificial Organs*, UPMC, http://www.upmc.com/SERVICES/REGENERATIVE-MEDICINE/RESEARCH/ARTIFICIAL-ORGANS/Pages/default.aspx [https://perma.cc/C79Q-3TAV] (last visited Nov. 2, 2017).

Cybersecurity Caucus, that would require devices purchased by the U.S. Government meet certain basic security requirements.[109]

V. WHEN THE TESTING IS OVER, YOU WILL BE MISSED

An adoption of this type of extensive software testing might be appropriate for certain agencies that deal with sensitive or critical devices. While U.S. Customs probably does not need to examine the software loaded on to an imported Keurig, the software controlling American vehicles probably should be subject to a higher level of scrutiny than it currently is. In particular, as self-driving cars become more prevalent on our highways and the internet of things further connects everyday electronics to our personal information, the need to thoroughly examine the behavior of the software that controls the behavior of regulated goods will increase.

There will not be a "one size fits all" approach for all federal agencies, but some amount of consideration of this problem is in order. Americans depend on the reliable operation of our electronics and that the U.S. Government is doing its best to ensure that they comply with all the relevant safety and operational standards. While specific agencies might choose to pursue their own software assurance schemes that are a better fit for their specific needs, it is clear that a national standards and assurance body would offer considerable value to US companies and consumers alike. This is particularly true if the formation and agenda setting is completed in partnership with the responsible government agencies. There will be drawbacks to this particular model, but they are far outweighed by the advantages that it would present.

109. Tetiana Tsukrova, *New IoT legislation to be introduced in U.S.*, THE STACK (Aug. 3, 2017, 5:55 PM), https://thestack.com/iot/2017/08/03/new-iot-legislation-to-be-introduced-in-u-s/ [https://perma.cc/QQ2N-BHY2].