Cybersecurity and Moral Hazard

Jeffrey L. Vagle*

23 STAN. TECH. L. REV. 67 (2020)

ABSTRACT

Our everyday lives are enmeshed, often invisibly, with connected technologies, making the security of those devices and the data they carry increasingly important. Yet our institutions have largely failed to address these technologies' cybersecurity risks. And that is in large part because they have failed to address—and have even exacerbated—the moral hazard inherent in making and selling connected technologies.

Currently, technology manufacturers, sellers, and service providers are richly rewarded for innovations that bring security risks, while technology users bear the bulk of the costs associated with those risks, including the nearly inevitable exploitation of their data. Technology manufacturers furthermore are positioned to understand and reduce those risks in ways technology users are not. And so technology manufacturers face a moral hazard: They must decide whether to make (or later fail to support) devices having risks that would be costly or impossible to eliminate for users—when those users will likely pay the same to them regardless.

Our institutions' support for technology innovation over product maintenance indulges rather than combats this moral hazard, especially in the low-margin business of connected devices and the Internet of Things (IoT). These failures are also due to our tendency toward technological ubiquity, the unclear—and often unhealthy—relationships between technology manufacturer and user, the inherent complexity of technology, and the network effects inherent to connected technologies.

This Article argues that this moral hazard leads to increased cybersecurity risks and will only be addressed when these categories, and their corresponding risks and costs, are

* Assistant Professor of Law, Georgia State University College of Law. The author would like to thank Steve Bellovin, Matt Blaze, Duncan Hollis, Chris Hoofnagle, Paul Ohm, Felix Wu, and the faculty at Penn State Dickinson Law School.

properly accounted for. The Article proposes changes to reduce the informational asymmetry between technology manufacturers and users, to better train software engineers to identify and resolve cybersecurity vulnerabilities, and to push companies to provide more secure devices, even or especially when cybersecurity risks are difficult or impossible to quantify.

TABLE OF CONTENTS

I. INTRODUCTION

The security of connected devices presents a unique moral hazard problem for which our current legal, political, technological, and economic institutions do not have good solutions.[1] The interconnected technological infrastructure we

1. For the purposes of this Article, I will define a "connected device" (or "connected technology") as any technology based around software or firmware with one or more methods of remotely accessing the device, e.g., through a network, through which some measure of control

have been building for the last fifty years or so—with a Cambrian explosion of growth taking place in the past two decades—has given modern societies enormous benefits, but has also left us with an ever-increasing dependency on fractally expanding systems of systems, the complexity of some of which are not completely understood by anyone, not even their designers.[2] If we are to accept this semi-blind dependency as an unavoidable component of the economic and social benefits we reap from systems of connected devices, we must also come to terms with the true costs associated with them, beginning with the imbalances of information and risk between the manufacturers of these technologies and their users, and the effects these imbalances have on their relationship and on society as a whole.

Discussion of the problem of moral hazard first arose in the context of insurance markets, where insurers worried about insuring people of poor character who would take advantage of the relationship by profiting from their own losses

---

of the device can be achieved. I will expand upon this concept further throughout this Article, but this basic definition will hold. Obvious examples of these devices include desktop and laptop computers, smartphones, computer servers, and network routers. Other, perhaps less obvious, examples include automobiles, refrigerators, electric meters, security and surveillance systems, smart watches, water flow meters, pacemakers, ATMs and point-of-sale devices, thermostats, pool cleaners, tractors, and even forks and cups. *See, e.g.*, *Vehicle to Vehicle Communications and Connected Roadways of the Future: Hearing Before the Subcomm. on Commerce, Mfg., and Trade of the H. Comm. On Energy & Commerce*, 114th Cong. (2015); Cho Mu-Hyun, *Samsung To Apply More AI, Voice Recognition to Smart Home Line-Up*, ZDNET (Aug. 22, 2017), https://perma.cc/9BG3-NA7R; Lisa Alejandro et al., *Global Market for Smart Electricity Meters: Government Policies Driving Strong Growth* (U.S. International Trade Commission, Working Paper, Jun. 2014); Marie Moe, *Go Ahead, Hackers. Break My Heart*, WIRED (Mar. 14, 2016), https://perma.cc/RCB5-6JEE; Tim Greene, *John Deere Is Plowing IoT Into Its Farm Equipment*, NETWORK WORLD (May 17, 2016), https://perma.cc/T92C-6YES; Valentina Palladino, *Hapifork Review: Eat Slower to Eat Better*, VERGE (Jan. 15, 2014), https://perma.cc/E8YT-Z7UC; Kyle VanHemert, *This Cup Tracks Exactly What You're Drinking with Molecular Analysis*, WIRED (Jun. 12, 2014), https://perma.cc/EPV6-3BCA. The explosive growth of connected devices plays a key role in my thesis, in that in their emerging ubiquity, the ecosystem created by these devices presents a sui generis moral hazard problem.

2. *See* KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET (1996) (tracing the early stages of networks and connected technologies from government science experiments to the early years of the Web); Rob van der Meulen, *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent from 2016*, GARTNER (Feb. 7, 2017), https://perma.cc/DHQ9-97FV; Louis Columbus, *Roundup of Internet of Things Forecasts And Market Estimates, 2016*, FORBES (Nov. 27, 2016), https://perma.cc/KQ5T-HTN8; Louis Columbus, *Internet of Things on Pace To Replace Mobile Phones as Most Connected Device in 2018*, FORBES (July 9, 2016), https://perma.cc/45BC-CHX6; Stephanie Condon, *Report: IoT to Dominate Connected Device Landscape by 2021*, ZDNET (Jun. 8, 2017), https://perma.cc/G263-68CB; Kavita Iyer, *Engineers Unable to Understand the Working of Google's Search AI*, TECHWORM (Mar. 10, 2016), https://perma.cc/FMY3-6AYA; Kalev Leetaru, *In Machines We Trust: Algorithms Are Getting Too Complex To Understand*, FORBES (Jan. 4, 2016), https://perma.cc/6BHU-42UJ; FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 6-10 (2015) (explaining the increasing use of complex algorithms in societal decision-making).

(at the insurer's expense).[3] Economists later generalized the concept of moral hazard to describe a market failure where the tendency of insurance (in the generic sense of the term) against costs associated with some risk can reduce the insured's incentives to minimize their risky activities.[4] Moral hazard finds especially fertile ground among relationships where information asymmetries exist between parties, giving the information-dominant party the opportunity to seek advantage by opaquely pushing the costs associated with their own risky actions to others.[5] Contemporary use of the term among economists (and those in adjacent fields) has grown to treat this problem as a market inefficiency to be corrected through monitoring or incentives, or some combination of the two, with light-touch, market-based solutions historically preferred; through such solutions, dysfunctional activities are to be identified, penalized, and—presumably—deterred.[6]

Of course, negative externalities, which are closely related to the problem of moral hazard, also play a role in the cybersecurity problem. Generally speaking, negative externalities arise when the costs—intended or unintended—of an activity are imposed on an unrelated third party.[7] Common examples of these external costs are pollution from burning coal, oil, and other fossil fuels;[8] excessive noise

3. *See generally* Tom E. Baker, *On the Genealogy of Moral Hazard*, 75 TEX. L. REV., 237-92 (1996).

4. *See* Kenneth J. Arrow, *Uncertainty and the Welfare Economics of Medical Care*, 53 AM. ECON. REV. 941 (1963); Mark V. Pauly, *The Economics of Moral Hazard: Comment*, 58 AM. ECON. REV. 531 (1968); Kenneth J. Arrow, *The Economics of Moral Hazard: Further Comment*, 58 AM. ECON. REV. 537 (1968); Mark V. Pauly, *Overinsurance and Public Provision of Insurance: The Roles of Moral Hazard and Adverse Selection*, 88 Q. J. ECON. 44 (1974); John M. Marshall, *Moral Hazard*, 66 AM. ECON. REV. 880 (1976); Bengt Hölmstrom, *Moral Hazard and Observability*, 10 BELL J. ECON. 74 (1979); Joseph E. Stiglitz, *Risk, Incentives and Insurance: The Pure Theory of Moral Hazard*, 8 GENEVA PAPERS RISK & INS. 4 (1983).

5. *See* Hölmstrom, *supra* note 4.

6. *See* Baker, *supra* note 3; Hölmstrom, *supra* note 4; John A. Nyman, *The Economics of Moral Hazard Revisited*, 18 J. HEALTH ECON. 811 (1999); Richard J. Arnott & Joseph E. Stiglitz, *Moral Hazard and Nonmarket Institutions: Dysfunctional Crowding Out of Peer Monitoring?*, 81 AM. ECON. REV. 179 (1991); Marta Fernandez-Olmos et al., *Double Sided Moral Hazard and Share Contracts in Agriculture*, 12TH CONG. EUR. ASSOC. AGRIC. ECONOMISTS (Aug. 26-29, 2008); H. Vetter, *Moral Hazard, Vertical Integration, and Public Monitoring in Credence Goods*, 29 EUR. REV. AGRIC. ECON. 271 (2002); Howard Beales et al., *The Efficient Regulation of Consumer Information*, 24 J.L. & ECON. 491 (1981); Michael Rothschild & Joseph Stiglitz, *Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information*, 90 Q.J. ECON. 629 (1976); Edward C. Prescott & Robert M. Townsend, *Pareto Optima and Competitive Equilibria with Adverse Selection and Moral Hazard*, 52 ECONOMETRICA 21 (1984); Stiglitz, *supra* note 4; Richard J. Arnott & Joseph E. Stiglitz, *The Basic Analytics of Moral Hazard*, 90 SCANDINAVIAN J. ECON. 383 (1988); Sarah Auster, *Asymmetric Awareness and Moral Hazard*, 82 GAMES ECON. BEHAV. 503 (2013); Deborah Stone, *Moral Hazard*, 36 J. HEALTH POL. POL'Y & L. 887 (2011); Leonard Kostovetsky, *Political Capital and Moral Hazard*, 116 J. FIN. ECON. 144 (2015).

7. *See* PAUL KRUGMAN & ROBIN WELLS, ECONOMICS 453-57 (3d ed. 2012).

8. *See* Richard A. Tybout, *Pricing Pollution and Other Negative Externalities*, 3 BELL J. ECON. & MGT. SCI. 252 (1972).

from production activities;[9] and health risks from industrial animal farming.[10] In these and similar examples, the economic benefits are realized by the producer of these activities, while the external costs are borne by third parties who may or may not see any of the benefits. In the realm of cybersecurity, negative externalities may arise through the increased risk of data theft or destruction, breaches of privacy, instability of connected infrastructures, or the overall impaired operation of connected technologies due to device vulnerabilities or lost trust.[11]

Of interest in this Article is a subspecies of moral hazard, the principal-agent problem, where risk sharing between the parties can lead to relationships that fall within the general insurer-insured category identified by economists as fodder for moral hazards.[12] In fact, a principal will often seek a relationship with an agent because of (rather than in spite of) an information asymmetry between the parties, with a common example being the relationship between firm owner (principal) and manager (agent), where the owner is forced to rely at least in part on an opaque understanding of the manager's actions.[13] As in other instances of moral hazard, the canonical approaches seek market solutions to resolve this market inefficiency.[14]

Our rapidly expanding connected device infrastructure, however, poses sui generis difficulties that recent history has shown cannot be solved by the usual market-based tweaks. It is difficult to overstate the scope of the cybersecurity problem with connected devices. Within the past decade, we have seen multiple examples of the reach connected technologies have throughout society, and the dangers inherent in the lack of basic security for many of these technologies.[15]

---

9. *See* Mats Wilhelmsson, *The Impact of Traffic Noise on the Values of Single-Family Houses*, 43 J. ENVTL. PLAN. & MGMT. 799 (2000).

10. *See* Jessica H. Leibler et al., *Industrial Food Animal Production and Global Health Risks: Exploring the Ecosystems and Economics of Avian Influenza*, 6 ECOHEALTH 58 (2009); Ellen K. Silbergeld et al., *Industrial Food Animal Production, Antimicrobial Resistance, and Human Health*, 29 ANN. REV. PUB. HEALTH 151 (2008); JoAnn Burkholder et al., *Impacts of Waste from Concentrated Animal Feeding Operations on Water Quality*, 115 ENVTL. HEALTH PERSP. 308 (2007).

11. See *infra* Part III.A.

12. *See* Steven Shavell, *Risk Sharing and Incentives in the Principal and Agent Relationship*, 10 BELL J. ECON. 55 (1979); David E.M. Sappington, *Incentives in Principal-Agent Relationships*, 5 J. ECON. PERSP. 45 (1991); Stephen A. Ross, *The Economic Theory of Agency: The Principal's Problem*, 63 AM. ECON. REV. 134 (1973); Mark A. Cohen, *Optimal Enforcement Strategy to Prevent Oil Spills: An Application of a Principal-Agent Model with Moral Hazard*, 30 J. L. & ECON. 23 (1987); Debi Prasad Mishra et al., *Information Asymmetry and Levels of Agency Relationships*, 35 J. MKT. RES. 277 (1998).

13. *See* Randy Silvers, *The Value of Information in a Principal-Agent Model with Moral Hazard: The Ex Post Contracting Case*, 74 GAMES & ECON. BEHAV. 352 (2012); Sappington, *supra* note 12.

14. *See* Silvers, *supra* note 13; Sappington, *supra* note 12.

15. Recent examples include the Russian cyber-attack on Georgia's Internet infrastructure, *see* John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES (Aug. 12, 2008), https://perma.cc/APG4-FB79, and Ukraine's electrical grid, *see* Andy Greenberg, *How an Entire Nation Became Russia's Test Lab for Cyberwar*, WIRED (Jun. 20, 2017), https://perma.cc/29NV-

Despite this, the connected device ecosystem of software, hardware, and protocols has historically been treated with a much lighter touch with respect to risk distribution and liability than in other manufacturer-consumer relationships, for a number of economic, legal, and social policy reasons which I will explore below.

This Article proposes five distinct, but complementary and nonexclusive, components to finding a better solution to the moral hazard of cybersecurity. First, we must work toward creating new, or enhance existing, incentives for manufacturers to build and maintain secure and reliable connected devices; second, we must do a better job of understanding and shrinking the information gap between technology manufacturer and technology consumer; third, we need an overhaul of our dated cost-benefit analysis when it comes to the software, hardware, and protocols of connected devices; fourth, we need to revisit the curricular requirements of software and hardware design and engineering programs; and fifth, we need to introduce a strong sense of justice and ethics into technology policy discussions.

Part II of this Article describes the concept of moral hazard, its origins, and its applicability to the problem of security of connected devices. Part III describes the unique moral hazard posed by cybersecurity issues, explaining why existing approaches to this problem are not sufficient. Part IV lays out the components I argue are necessary for a full and fair solution to cybersecurity's moral hazard problem.

II. THE CONCEPT OF MORAL HAZARD

A. Origins and Generalization of the Term

The original concept of the term "moral hazard" can be found in nineteenth-century insurance markets, where it emerged out of the use of probability theory to establish a "doctrine of chances" necessary for calculating the odds upon which emerging insurance companies depended to remain profitable.[16] The Victorian

NDFH; the massive security flaws found in electronic voting machines, *see* Kim Zetter, *The Crisis of Election Security*, N.Y. TIMES (Sept. 26, 2018), https://perma.cc/MC7A-TDR2; the theft of sensitive election materials by Kremlin-linked hacker groups, *see* Kevin Poulsen, *Mueller Finally Solves Mysteries About Russia's 'Fancy Bear' Hackers*, DAILY BEAST (Jul. 20, 2018), https://perma.cc/6TK4-EAVH; the security vulnerabilities in modern automobiles, *see* Andy Greenberg, *A Deep Flaw in Your Car Lets Hackers Shut Down Safety Features*, WIRED (Aug. 16, 2017), https://perma.cc/7NP8-C2KT; security flaws in autonomous vehicles, *see* Nicole Perlroth, *Electronic Setups of Driverless Cars Vulnerable to Hackers*, N.Y. TIMES (Jun. 7, 2017), https://perma.cc/5GFK-QN73; software vulnerabilities in our smartphones, *see* Charlie Osborne, *25 Android Smartphone Models Contain Severe Vulnerabilities Off the Shelf*, ZDNET (Aug. 13, 2018), https://perma.cc/427N-XFA2; just to name a few in a long, and growing, list.

16. *See* Baker, *supra* note 3, at 244-46. Interestingly, the name given to those who applied probability to calculate odds of those natural (and unnatural) life events of interest to insurers was "moral scientist." These moral scientists were named for their hubristic hope that they

ideal of the moral person became inevitably enmeshed in the language of insurance, as insurers sought as customers only those who were upright, honest, thrifty, and hardworking.[17] Those of lesser moral standing brought with them greater risk, as their lowly character included the unwanted characteristics of intemperance, carelessness, improvidence, sloth, and uncleanliness, and therefore presented insurance companies with increased probabilistic risk.[18] Thus, just as there are "physical hazards" that can cause accidents and loss, insurers took into consideration the "moral hazards" presented by those considered less upstanding and trustworthy: poor character and bad habits led to the increased odds of loss.[19] Insurers also realized, however, that this moral hazard could quite easily extend beyond those of low moral character, and the very fact that the insured was protected from the vagaries of chance could very well cause that person to take on additional, and unnecessary, risk.[20] Moral risk therefore came to mean not only the risks inherent in insuring "immoral" people, but also the perverse incentives made possible by the very concept of insurance.[21]

In the 1960s, the law and economics movement adapted the concept of moral hazard to the general notion of rational responses to incentives, dispensing with the moral principles and judgments previously associated with the term.[22] In other words, the economic interpretation of moral hazard—which has since become the conventional wisdom on the topic—applies the *homo economicus* assumption, where people are rational, self-interested agents who seek to minimize loss and maximize gain, and will therefore behave differently when the risks and consequences of their actions can be shifted to others.[23] While the concept of moral hazard is still firmly rooted in insurance analysis, its effects have spread to

might predict the future "of moral as well as of physical phenomena," thus reducing life to a complicated game that could, nonetheless, be tamed through the mathematics of chance. *Id.* at 247.

17. Baker, *supra* note 3, at 249.

18. *Id.* at 249-50.

19. *Id.* at 248-49.

20. *Id.* at 250-52.

21. *Id.* at 251.

22. The adaptation (and adoption) of the concept of moral hazard by economic theorists can be traced to Arrow, *Uncertainty*, *supra* note 4, wherein Arrow analyzed the economics of health insurance and health care, and linked the availability of privately purchased health insurance with the increased use of medical services, which resulted in higher costs for those services over time. Arrow concluded by recommending the government provision of health insurance to mitigate the moral hazard created by private health insurance. Mark Pauly responded to Arrow by pointing out that moral hazard had very little to do with morality, but instead described rational responses to economic incentives. Pauly, *Comment*, *supra* note 4. Arrow's response to Pauly included the pointed criticism that "rational economic behavior" and "moral perfidy" are not mutually exclusive concepts, stating "[n]o doubt Judas Iscariot turned a tidy profit from one of his transactions, but the usual judgment of his behavior is not necessarily wrong." Arrow, *Further Comment*, *supra* note 4, at 538.

23. *See* Pauly, *Comment*, *supra* note 4.

areas of scholarship as far afield as products liability, welfare, banking, corporations, and workers' compensation.[24] Across these areas, law and economics concludes that moral hazard is economically inefficient.[25] A problem with this analysis, however, lies in the fact that moral hazard is based on a social construction, and not economic absolutes.[26] When we assert that moral hazard is either an overall good or bad for society, we are basing that assumption on value judgments about what behaviors should—and should not—be protected or subsidized. This issue becomes evident when one examines the early economics literature on the concept of moral hazard.

Economists' use of the concept of moral hazard can be traced to the vigorous and enlightening exchange in the early 1960s between Ken Arrow and Mark Pauly. Arrow's 1963 analysis of the economics of health care in the United States brought the concept of moral hazard out of the narrow confines of insurance into a broader and more generalized law and policy debate.[27] In his article, Arrow defined the moral hazard in health insurance as "the effect of insurance on incentives," arguing that the government provision of health insurance would alleviate the temptation for the privately insured to base their medical choices not on actual need, but rather on a particular medical professional's willingness to charge costlier procedures to their insurer.[28] Pauly's challenge to Arrow's analysis questioned his use of the term "moral hazard" to describe rational economic decisions that had "little or nothing to do with morality," and called for a market, rather than a governmental, solution.[29] Arrow's concise response to Pauly highlights a critical difference in schools of economic thought, to which I will return later in this Article.[30] Specifically, Arrow challenged Pauly's assertion that "rational economic behavior" and "morality" are mutually exclusive, pointing out that healthy economic systems depend on "the relations of trust and confidence between principal and agent," so that "the agent will not cheat even though it may be 'rational economic behavior to do so.'"[31]

---

24. *See* Keith N. Hylton, *The Law and Economics of Products Liability*, 88 NOTRE DAME L. REV. 2457 (2013); Martha T. McCluskey, *Efficiency and Social Citizenship: Challenging the Neoliberal Attack on the Welfare State III. General Matters*, 26 WORKERS' COMP. L. REV. 425 (2004); Arthur E. Wilmarth, Jr., *The Transformation of the U.S. Financial Services Industry, 1975-2000: Competition, Consolidation, and Increased Risks*, 2002 U. ILL. L. REV. 215 (2002); Christopher M. Bruner, *Corporate Governance Reform in a Time of Crisis*, 36 J. CORP. L. 309 (2011); Martha T. McCluskey, *The Illusion of Efficiency in Workers' Compensation "Reform,"* 50 RUTGERS L. REV. 657 (1998).

25. *See* Pauly, *Comment*, *supra* note 4.

26. *See* Arrow, *Further Comment*, *supra* note 4.

27. *See* Arrow, *Uncertainty*, *supra* note 4.

28. *See id.*

29. *See* Pauly, *Comment*, *supra* note 4, at 535.

30. See *infra* Part II.C.

31. *See* Arrow, *Further Comment*, *supra* note 5. In fact, Arrow's rebuke of Pauly's "morality-free" rationality argument was rather pointed, wherein he wrote that "Mr. Pauly's wording suggests that 'rational economic behavior' and 'moral perfidy' are mutually exclusive categories.

Beyond raising this (not unimportant) disagreement, the initial result of this exchange for economists was that moral hazard became defined as relying on the *homo economicus* assumption that people are, above all else, rational minimizers of loss, and will therefore react to the existence of insurance by taking more risks, with the potential costs of those risks being shifted from the insured to the insurer.[32] The early economist's version of moral hazard thus removed the concept of moral character from the insurer's model, effectively mapping the old idea of the moral vice of temptation to the more modern economic theory of incentives, exchanging a theory of moral choice for one based almost solely on cost-benefit analysis.[33] I argue that this school of thought is not necessarily wrong, but incomplete; it provides insufficient purchase to properly grapple with the moral hazards posed by the security of connected devices.[34] The scale and distribution of risks for these novel technologies cannot be easily quantified or predicted, a point the cost-benefit approach fails to grasp; a more robust approach would join quantitative and qualitative analysis, using principles to guide decisions amidst the levels of uncertainty related to technology's inherent complexities.

What makes moral hazard a much more general concept than the narrower version that originated among insurers is the fact that the problem arises whenever the costs attributable to one party's risks are borne by another.[35] Because such a situation is almost always accompanied by moral hazard, scholars have long applied various cost-benefit models to the moral hazards that can occur under these conditions, seeking solutions of Pareto-optimal risk sharing in order to limit the incentives for one or the other party to cheat by unfairly benefiting from risky actions while the costs of those actions are shifted elsewhere. But in order to calculate this optimal solution, economists must first make certain assumptions as to the liabilities and protections to which the parties in this relationship are entitled. That is, finding the optimal transfer of risk that minimizes moral hazard requires the construction of a metric, which is in turn built upon a set of value judgments about appropriate compensation and liability structures.

No doubt Judas Iscariot turned a tidy profit from one of his transactions, but the usual judgment of his behavior is not necessarily wrong." *Id.* at 538.

32. *See* Arrow, *Uncertainty*, *supra* note 4; Pauly, *Comment*, *supra* note 4; Arrow, *Further Comment*, *supra* note 4; Richard Zeckhauser, *Medical Insurance: A Case Study of the Tradeoff Between Risk Spreading and Appropriate Incentives*, 2 J. ECON. THEORY 10 (1970); Pauly, *Overinsurance and Public Provision of Insurance*, *supra* note 4; Marshall, *supra* note 4; Stiglitz, *supra* note 4.

33. *See* Pauly, *Overinsurance and Public Provision of Insurance*, *supra* note 5; Hölmstrom, *supra* note 4; Stiglitz, *supra* note 4.

34. *See infra* Part III.A.

35. This is, of course, a general definition of insurance, which Stiglitz pointed out is a much more universal concept than the idea of specific insurance regimes, such as health, fire, automobile, marine, etc. *See* Stiglitz, *supra* note 5, at 8.

B. Information Asymmetries as a Fulcrum of Moral Hazard

As Arrow, Pauly, and others have long pointed out, the search for optimal risk distribution can be quickly derailed by information imbalances between parties.[36] If one of the parties in the risk relationship can privately take actions that are opaque to others and yet change the likelihood of costs or benefits materializing to other parties from the relationship, a Pareto-optimized solution is often unavailable due to the corruption of the incentive model upon which an optimal solution depends.[37] The classical economic model supposes all parties in a risk-sharing relationship have comparable levels of awareness of the risks and cost probabilities associated with their relationship. That model quickly loses relevance when one party has a more complete understanding and control of the relationship's uncertainties—and thus can exploit them.

In fact, information asymmetry is the relational catalyst of the moral hazard problem.[38] An information imbalance regarding the probabilities and costs in any risk sharing relationship presents the opportunity (and temptation) for the information dominant party to take cost-shifted risks or otherwise "cheat" the shared understandings of the parties' relationship.[39] I do not wish to assert, of course, that economic relationships are not accompanied by risk or require perfect information symmetry to succeed—this would be impractical even if we assume good faith and risk neutrality on the part of all parties in all such relationships.[40] The existence of information imbalances and associated risk is, indeed, baked into the standard economic model of competitive analysis, and conventional wisdom holds that, while true competitive equilibria may not exist under these conditions, various corrective measures exist to minimize the effects of these market inefficiencies.[41]

The problem of information imbalances is well illustrated in a special case of the moral hazard problem, the principal-agent relationship, as these relationships nearly always require nontrivial risk sharing coupled with information asymmetries between the parties. In these relationships one of the parties (the principal) needs to rely upon the other (the agent) for some desired result where information regarding the effort of the agent is not immediately observable to the principal (for any number of reasons). A canonical example of this relationship is that of the

---

36. *See* Arrow, *Uncertainty*, *supra* note 4; Pauly, *Comment*, *supra* note 4; Arrow, *Further Comment*, *supra* note 4.

37. *See* Hölmstrom, *supra* note 4; Sappington, *supra* note 12.

38. *See* Hölmstrom, *supra* note 4; Stiglitz, *supra* note 4; Arnott & Stiglitz, *Basic Analytics*, *supra* note 6.

39. There are, of course, methods through which moral hazard due to information asymmetries can be mitigated. I address this topic above in Part IV.

40. Indeed, the study and use of game theory and related models arose to understand parties' decisions based on their interests and motivations. *See, e.g.*, Sappington, *supra* note 12; Shavell, *supra* note 12; Nyman, *supra* note 6; Stiglitz, *supra* note 4; Prescott & Townsend, *supra* note 6; Rothschild & Stiglitz, *supra* note 6.

41. *See infra* Part IV.C.

business owner (principal) who delegates the responsibilities of running her business to a manager (agent) for reasons of both available time and expertise. Because the owner does not generally have the ability to monitor the manager's actions—the freedom from the day-to-day decisions is a big part of the reason behind her choice to delegate these tasks to the manager—a moral hazard problem arises. The owner may be unable to discern whether the company's good (or poor) performance is due to the manager's actions or just good (or bad) luck. And so, if the owner rewards the manager with a bonus tied to the firm's performance, the manager may be tempted to make riskier business decisions based on the "insurance" the firm provides that protects him from the costs of bad risks while rewarding him when the risks pay off.

A more relevant example of this principal-agent problem (to this Article, at least) is found in the risk-sharing relationship that exists between manufacturer and consumer. When consumers select a particular good from a manufacturer, they are presumably making that decision based on their knowledge of the quality of the good. More often, however, consumers only maintain information about the average quality of goods in a category rather than information regarding a specific manufacturer's product.[42] For some products, consumers are unable to make judgments as to their quality until they actually use that product.[43] In fact, there is yet another category of good ("credence goods") within which consumers cannot judge the products' quality even after its purchase or consumption.[44] When consumers (the principals in this model) cannot assess a product's quality before purchase, they are also unable to evaluate any investments the manufacturer (the agent) may have made toward the quality and safety of their product, and are thus on the short end of an information asymmetry with respect to risk distribution; this presents an inevitable manufacturer moral hazard. That is, agent-manufacturers may take advantage of this information asymmetry by reducing investments in their products' safety and quality down to the point where the effects are noticed by the consumer, thus reaping the benefits of lowered manufacturing expenses while pushing the costs of the risks associated with those lowered expenses onto the consumer.

---

42. *See* Steven P. Croley & Jon D. Hanson, *Rescuing the Revolution: The Revived Case for Enterprise Liability*, 91 MICH. L. REV. 683, 707-08 (1993); Beales et al., *supra* note 6.

43. *See* Phillip Nelson, *Information and Consumer Behavior*, 78 J. POL. ECON. 311 (1970). Nelson distinguished "search goods" (those products that consumers can examine for quality prior to purchase) and "experience goods" (products for which consumers cannot observe their quality until they purchase or consume them). *Id.*

44. The term was first introduced by Darby and Karni in 1973 to describe a product's qualities "which, although worthwhile, cannot be evaluated in normal use." Michael R. Darby & Edi Karni, *Free Competition and the Optimal Amount of Fraud*, 16 J. L. & ECON. 67, 68-69 (1973). The classical example of this category are medical services, legal services, and automobile repairs, where one party—the expert—is contracted by the consumer to both provide the good but also judge just what—and how many—goods the consumer actually needs.

This is not a new problem, of course, and addressing this particular moral hazard problem is generally accomplished through tort or contract, where manufacturers face some degree of liability for consumer injuries due to their product. But what rule (or rules) need to be in place to address a products liability moral hazard problem in a maximally efficient manner? If we hold manufacturers completely liable for the costs of injuries from their product, this reduces the consumer's incentive to avoid the risks that might lead to those injuries. On the other hand, limiting a manufacturer's liability transfers the costs of product risk to consumers. The two primary tools used to address this two-sided moral hazard problem have long been contract and tort rules, with an ongoing push and pull between schools of thought regarding the most efficient, effective, or just method of resolution. As with other moral hazards, a central component to this analysis is the problem of information asymmetry that exists between manufacturer and consumer. More specifically, competing theories on the proper resolution of products liability moral hazard problems seek to account for these natural information imbalances by adjusting the balance of risk—and liability for the costs associated with that risk—between the parties.

The tools available for resolving the consumer-manufacturer moral hazard problem are generally limited to those used in modern products liability doctrine, specifically tort and contract law, where the dominant school of thought seeks to use these tools instrumentally in the quest for economic efficiency. Optimal solutions to moral hazard under this theory are designed to find the least-cost avoider to arrive at a market efficient solution. For example, if a manufacturer is held fully liable for consumer injuries from their products by the terms of the product's warranty, they will tend to maximize their spending on product safety. But even under these conditions, products will still fail from time to time, and the manufacturer will be held contractually responsible for the accompanying injuries. This is an economically inefficient arrangement, as it requires the manufacturer to make suboptimal investments in product safety and forces the manufacturer to fully insure the consumer, even if the manufacturer is not in the best economic position to compensate for the product failure.

C. Resolving Moral Hazard Problems

The articulation beginning with Arrow, Pauly, and others, on the potential for moral hazard in any relationship where one party is able to shift the costs associated with their risk onto other parties, is naturally accompanied by recommendations for solving or mitigating these problems by correcting information imbalances, adjusting incentives, or some combination of the two. For instance, a common solution is that of increased observability, where parties are expected to submit to some kind of monitoring regime that rewards the reasonable sharing of information and punishes unfair behaviors. Common examples of such monitoring schemes include the requirement of regular reporting or the performance of audits or inspections, either by one of the parties or a trusted third party, such

as a government agency.[45] In the principal-agent variant of the moral hazard problem, where the presumption of rational self-interest on the part of all parties is generally fixed, game theoretic approaches seek an optimal risk distribution based on variables including the parties' respective aversions to risk, the probabilities and costs of inherent risks, the costs of risk avoidance, the levels of insurance (in the generic sense articulated above), and information flow (or lack thereof) in order to highlight pressure points—in the form of information and/or incentives—which can be adjusted to derive optimal distributions of risks and incentive effects.

Successful methods of resolving moral hazard, both theoretically and empirically, can be found in one or more of the following categories:

1. Market-based approaches;
2. Policies and forcing functions;
3. Public monitoring;
4. Private monitoring (internal and external).[46]

While each of these categories are derived from differing legal and political foundations, they all share a requirement that information asymmetries are either directly corrected or indirectly compensated, e.g., through contract incentives and disincentives. Further, these solution categories are often applied in tandem, depending on the particulars of the moral hazard problem presented.

Market solutions to moral hazards are those that seek a presumed equilibrium based on some expected utility function applied by each of the players, i.e., the insured and the insurer(s).[47] Based on economic models such as those proposed by Arnott, Stiglitz, Demski, Sappington, and others, these solutions tend to be the least invasive in that they rely on the rational economic choices of the parties to correct the market failure that is moral hazard by adjusting the terms of their agreements accordingly.[48] Potential weaknesses of this approach include its

45. *See, e.g.*, Vetter, *supra* note 6 (illustrating how public monitoring can alleviate moral hazard caused by information asymmetries); Prescott & Townsend, *supra* note 6 (exploring use of market optimization analysis to economies where unobserved actions can lead to moral hazard); Darby & Karni, *supra* note 44 (examining the problem of fraud due to moral hazard of information asymmetry between seller and buyer, and use of market efficiencies to alleviate this problem); Joel S. Demski & David E.M. Sappington, *Resolving Double Moral Hazard Problems with Buyout Agreements*, 22 RAND J. ECON. 232 (1991) (discussing use of pre-negotiated contract terms to avoid moral hazard fallout).

46. E.g., peer monitoring, *see* Arnott & Stiglitz, *Moral Hazard and Nonmarket Institutions*, *supra* note 6.

47. *See, e.g.*, Stiglitz, *supra* note 4.

48. By far the most popular medium of resolution in this category is that of contract, where parties are expected to adjust their terms accordingly. *See, e.g.*, *id.* (applying use of differing contract terms depending on levels of information asymmetry between parties to avoid moral hazard); Auster, *supra* note 6, at 503-21 (seeking optimal contractual arrangements between parties to reduce information asymmetries); Silvers, *supra* note 13 (appropriate contract terms between principal and agent where different levels of information may be available); Prescott & Townsend, *supra* note 6 (discussing use of contracts meant to optimize markets to

failure to take into account the weight of a particular actor's market power relative to the others in the transaction, or an overreliance on rational choice theoretic assumptions.[49]

Toward the other end of the intrusiveness spectrum we find policy solutions that add forcing functions to the existing economic model in order to provide corrections to a market failure caused by information imbalances.[50] These solutions may be regulatory or legislative in nature, but can also rely on the modification of legal doctrines such as those of tort and contract law.[51] Criticisms of these approaches often originate from free market proponents, who argue that increasingly intrusive approaches can create more inefficiencies than they resolve.[52] These approaches can thus meet resistance from manufacturing and other corporate interests, who balk at the addition of regulatory or legal frameworks to otherwise open markets.[53]

Given the fact that information asymmetries are almost always at the root of moral hazard problems, remedies that include some form of monitoring arise as

reduce moral hazard); Demski & Sappington, *supra* note 45. For example, if an owner of an enterprise wishes to ensure that their agent is performing with the owner's interest in mind, they can include a term in their agreement that could force the agent to buy out the enterprise, thus ensuring the agent will work toward maximizing the value of that enterprise. Demski & Sappington, *supra* note 45, at 233-34.

49. In fact, an entire field of economic theory has arisen around objections to a perceived overreliance by classical economists on the assumption of the rational actor of *homo economicus*. Behavioral economics applies research from fields such as psychology, sociology, and anthropology to derive a more comprehensive—and presumably more accurate—picture of human and organizational decision making. *See, e.g.*, Cass R. Sunstein et al., *A Behavioral Approach to Law and Economics*, 50 STAN. L. REV. 1471 (1998). Behavioral economists therefore argue that classical economic solutions to adjust for market failures such as moral hazard often fall short due to the fact that they do not properly account for a person's revealed preferences, which do not always comport with economic models of rational choice. *See* Richard H. Thaler & Cass R. Sunstein, *Libertarian Paternalism*, 93 AM. ECON. REV. 175, 176-78 (2003).

50. A relatively recent example of this approach can be found in the moves to provide additional regulation of investment and banking firms in the wake of the 2008 financial crisis. *See, e.g.*, Troy Brown, *Legal Political Moral Hazard: Does the Dodd-Frank Act End Too Big to Fail?*, 3 ALA. C.R. & C.L. L. REV. 1 (2012).

51. The core concept is not recent, however, and can be found in the many discussions around tort law, especially versus contract, as an efficient means of adjusting inefficiencies such as moral hazard. *See, e.g.*, George L. Priest, *Strict Products Liability: The Original Intent*, 10 CARDOZO L. REV. 2301 (1989); Mark Geistfeld, *Manufacturer Moral Hazard and the Tort-Contract Issue in Products Liability*, 15 INT'L REV. L. & ECON. 241 (1995); David G. Owen, *The Moral Foundations of Products Liability Law: Toward First Principles*, 68 NOTRE DAME L. REV. 427 (1993).

52. *See, e.g.*, Omri Ben-Shahar & Kyle D. Logue, *Outsourcing Regulation: How Insurance Reduces Moral Hazard*, 111 MICH. L. REV. 197 (2012); Kevin Dowd, *Moral Hazard and the Financial Crisis*, 29 CATO J. 141 (2009).

53. *See, e.g.*, Darby & Karni, *supra* note 44; Barry J. Nalebuff & Joseph E. Stiglitz, *Prizes and Incentives: Towards a General Theory of Compensation and Competition*, 14 BELL J. ECON. 21 (1983); Adam Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J. L. & TECH. 6 (2015).

natural solutions.[54] Such monitoring schemes can be private (e.g., through contract terms), public (e.g., conducted by regulatory agencies), or quasi-public (e.g., via private watchdog organizations). Their perceived acceptability tends to coincide with where one lies on the free market vs. regulation continuum.

In the following Part, I will explain why historically successful approaches to resolving moral hazard are insufficient to address the specific problems raised by the security of connected devices. Specifically, I will lay out why cybersecurity's moral hazard—and its principal-agent problem—are different enough to require a new way of resolving these problems.

III. CYBERSECURITY'S SUI GENERIS PRINCIPAL-AGENT PROBLEM

What makes connected devices specifically, and software generally, different is twofold: how they operate, and *how much* they actually do, much of which is unbeknownst to their users. Computer servers that used to occupy the space of a large refrigerator and require three-phase power, air conditioning, and highly specialized administrators to manage them now easily fit into the palm of your hand, can plug into any wall socket, will sit unnoticed on your desk, and are orders of magnitude less expensive—and still they can run computational circles around the behemoths of just 20 or 30 years ago.[55] The rapid and remarkable shrinking of device cost and size, coupled with the explosive growth of their availability, has yielded a commodification of computers and a focus on software that has prompted technology experts to proclaim that "software is eating the world," a phrase that serves both as triumphant exclamation and dire warning.[56] That is, the emergence of a software-driven economy and society has yielded great benefits while also burdening us with very real and complex dangers. This not only presents a problem in the sheer numbers of connected devices, but also in the number of software-based functions—many hidden from their users—that each of these devices offers.

A. The Unique Technological Characteristics of the Problem

In order to introduce the assertion that the security of connected technologies presents a unique set of information asymmetries that yield a particularly difficult moral hazard problem, it is helpful to begin with an example. The hidden

54. *See* Arnott & Stiglitz, *Moral Hazard and Nonmarket Institutions*, *supra* note 6; Vetter, *supra* note 6; Beales et al., *supra* note 6.

55. *See, e.g.*, *Building a Tiny Server*, INSTRUCTABLES, https://perma.cc/2LUQ-MQAV (archived Dec. 12, 2019) (providing an example of ease and low cost of building a tiny computer server); DECsystem 5500 Brochure, DIGITAL EQUIPMENT CORPORATION, https://perma.cc/PJF8-73L3 (Aug. 1991) (providing a typical illustration of the size, complexity, and expense of microcomputers of 1980s-90s).

56. *See* Marc Andreessen, *Why Software Is Eating the World*, WALL ST. J. (Aug. 20, 2011), https://perma.cc/92J5-Z6Y7.

functionality problem can be found in the basic Calendar application that is included with the base Android operating system.[57] As with other calendar and scheduling applications, there are a number of basic functions that this application should provide to the user, such as event creation and reminders, as well as other features we have grown used to over the years, including integration with email and reservation applications. But while these functions may seem elementary to the user of the application, the code behind the scenes tells another, more complex, story. Examining the functional source code for the Calendar application, we find that there is a total of

- 108 Java files;
- 281 XML files;
- 34,294 lines of Java source code; and
- 35,800 lines of XML source code.[58]

In addition to this source code, the Calendar application must rely upon other "libraries" of software that come with, or are built into, the Android operating system and provide much of the basic functionality, such as touch screen interaction, access to local files, network connectivity, and so on.[59] These libraries, in turn, are compiled from thousands of other source code files and contain millions of lines of code.[60] All of this code is necessary for our Calendar application to provide its basic user functionality while hiding the bulk of its full range of functions from the user. One does not have to be a software developer to understand how the hidden size and complexity of software can quickly explode with applications that are functionally far beyond the lowly Calendar application.

The problem of complexity has always been directly intertwined with the design and realization of the software and hardware behind connected technologies.[61] For the most part, this problem has roots in the external complexities of

57. *See Android Calendar Source Code Repository*, GITHUB, https://perma.cc/TW2S-XV62 (archived Dec. 12, 2019). For the purposes of this example, I will be referring to version 7.0 of the application, which ships with Android 7.0 ("Nougat").

58. Briefly, Java is a software programming language used by Google to write much of their Android operating system and applications. *See Java Language and Virtual Machine Specifications*, ORACLE, https://perma.cc/C8XC-Q2YB (archived Dec. 12, 2019). File and line counts, by themselves, are poor indicators of complexity, but they do give the reader an idea of the difficulty in coding, maintaining, and updating even the most rudimentary (from the user's point of view) of user applications.

59. *See* HISTORY OF PROGRAMMING LANGUAGES 369 (Richard L. Wexelblat ed., ACM monograph series, 1st ed. 1981) (describing early development of software library concept as a method of separating functional concerns and hiding information).

60. *Id.*

61. As Frederick Brooks so succinctly put it, "The complexity of software is an essential property, not an accidental one." FREDERICK P. BROOKS, JR., THE MYTHICAL MAN-MONTH: ESSAYS ON SOFTWARE ENGINEERING 183 (2d ed. 1995). *See also* P.F. CALDER, SOUTH AUSTRALIAN DEPARTMENT OF DEFENCE ELECTRONICS RESEARCH LABORATORY, MANAGING SOFTWARE COMPLEXITY (1986), https://perma.cc/YMC6-F7RZ; Rajiv D. Banker et al., *Software Development Practices, Software Complexity, and Software Maintenance Performance: A Field Study*, 44 MGMT.

the problems connected technologies are trying to model and solve.[62] For example, the ability of our smartphones to seamlessly connect, disconnect, and reconnect to cellular networks requires an incredibly intricate system of radio frequency hopping, voice and data channel management, and back end administration to work, which it usually does without the user having to think twice about it.[63] Hiding this complexity from the user is the point of connected technology design—managing complex problems for the user by masking complexity within a black box is a large part of what makes these technologies useful (and usable) to the consumer.

Since information asymmetries lie at the core of moral hazard, it should come as no surprise that technologies designed and built to conceal their inner workings to their users would lead to such problems. Imbalances of information between parties is nothing new to those examining the problem of moral hazard, of course, but connected devices are decidedly different from other sources of this problem for three reasons. First, the black box approach acts as both feature and bug, as it encourages conscious and willful technological blind spots on the part of users ("I'm just not a technology person"), allowing manufacturers the option of shifting the risks associated with technological complexity to the user.[64] Second, the complexities hidden by the black box approach are, from the nature of the problems they are solving as well as the nature of software itself, often orders of magnitude greater than those we have seen in past technologies, making the risk of vulnerabilities near certain.[65] Third, the unpredictably interlinked nature of connected technologies—sometimes by design, often by accident—creates complex dependencies that puts these devices in a risk category by themselves.[66]

Largely because of connected technologies' inherent differences from other categories of products and/or services, the usual methods of resolving the moral risks attendant in information asymmetries associated with connected technologies have not been effective in balancing manufacturer-consumer risks in either the moral or ethical senses that serve as the bases for resolving moral hazard.[67]

SCI. 433, 433-50 (1998); Jeff Kramer & Orit Hazzan, *The Role of Abstraction in Software Engineering*, PROC. 28TH INT'L CONF. ON SOFTWARE ENGINEERING 1017 (2006); Rajiv D. Banker et al., *Software Complexity and Software Maintenance Costs*, 36 COMM. ACM 81 (1993).

62. *See* Ned Chapin, *A Measure of Software Complexity*, 1979 INT'L WORKSHOP ON MANAGING REQUIREMENTS KNOWLEDGE 995 (illustrating importance of measuring both extent and source of software complexity).

63. *See* George Lawton, *What Lies Ahead for Cellular Technology?*, 38 COMPUTER 14 (2005) (describing technological advances taken through subsequent generations of cellular services).

64. *See* Richard Warner & Robert H. Sloan, *Vulnerable Software: Product-Risk Norms and the Problem of Unauthorized Access*, 2012 U. ILL. J.L. TECH. & POL'Y 45 (2012); Silvers, *supra* note 13; Geistfeld, *supra* note 51.

65. *See* Eric Bonabeau, *Understanding and Managing Complexity Risk*, 48 M.I.T. SLOAN MGMT. REV. 62 (2007).

66. *See, e.g.*, *id.*

67. I will return to the concept of the moral and ethical bases for resolving moral hazard

Some of this is due to the inherent difficulties of correcting connected device information imbalances, where the underlying problem being solved is so complex that a complete, or even working, understanding of the technology by the consumer is impossible.[68] A significant portion of this problem, however, is artificial, and can be attributed to the legal and policy decisions we have made with respect to the technological advances brought by computer hardware and software over the past half century or so.

1. Technological Ubiquity and Invisibility

Look around you. It is likely that you are currently surrounded by connected technologies.[69] In fact, it is possible that you are reading this on such a device right now.[70] But perhaps you are reading this on paper in a secluded copse that you specifically sought out to get away from the technologies I refer to. Even in this case, it is probable that you have a smart phone within arm's reach, and even if you don't have cellular coverage where you currently sit, those "dark" spaces are shrinking every year.[71] In fact, we are now so often in the presence of—and dependent upon—connected technologies that we tend to ignore them as "technologies," and instead consider them everyday tools or commodities, if we consider them at all.[72] There are clear benefits to this explosion of connected technologies, of course. The possibilities for economic and social advancement created by and through remote medicine, driver-assisted vehicles, global positioning, and instantaneous communications seem never-ending. But there are down sides to this Cambrian explosion of connected technologies, as well, not least of which are the risks associated with the malicious manipulation of these devices and their associated networks, resulting in the theft or loss of private information, hijacking of device functions, and in an increasing number of cases, physical damage and the endangering of human lives.[73]

---

problems later in this Article. For an excellent introduction to the concept generally, see Owen, *supra* note 51; David G. Owen, *The Intellectual Development of Modern Products Liability Law: A Comment on Priest's View of the Cathedral's Foundations*, 14 J. LEGAL STUD. 529 (1985); Priest, *supra* note 51.

68. *See, e.g.*, Lawton, *supra* note 63 and accompanying text.

69. *See* note 1, *supra*, and accompanying text.

70. *See* Andrew Perrin, *Majority of Americans Are Still Reading Print Books*, PEW RES. CTR. (Sept. 1, 2016), https://perma.cc/QEM6-PR3X.

71. *See* KALVIN BAHIA, GSM ASS'N, CONNECTED SOCIETY: STATE OF MOBILE INTERNET CONNECTIVITY 2018 (2018); Dave Anderson, *Mobile Network Performance in the US*, ROOTMETRICS (Feb. 18, 2016), https://perma.cc/C89A-4WFM.

72. *See* Arun Kumar Tripathi, *Reflections on Challenges to the Goal of Invisible Computing*, 2005 UBIQUITY 1 (2005) (exploring the ethical considerations relating to invisible computing).

73. *See* Jack Wallen, *Five Nightmarish Attacks That Show the Risks of IoT Security*, ZDNET (Jun. 1, 2017), https://perma.cc/G7QR-6GPP.

These risks, once considered remote or trivial, have now become very real and serious facets of modern life.[74] Further, as our world becomes more and more dependent on connected technologies, we expose ourselves to greater risks that may one day outweigh the benefits of these technologies.[75] One might ask why this must be the case. Throughout modern history, as new technologies have presented risks, we have taken steps—technological, social, legal—to mitigate those risks.[76] Why should connected technologies be any different?

A significant part of the answer to this question lies in the increasing invisibility of connected technologies in our daily lives. This has long been a goal for manufacturers of connected technologies, reasoning (correctly) that users do not want to be exposed to the increasingly complicated workings of their devices, and would rather purchase technologies that "just work."[77] But good design should also take into account the safety and reliability of the technology, features that are often pushed far down the design priority queue due to costs, lack of appropriate resources, aesthetics, and user resistance.[78]

---

74. *See How To Manage the Computer-Security Threat*, THE ECONOMIST (Apr. 8, 2017), https://perma.cc/5GF9-QYCL.

75. *See* Steve Rayner & Robin Cantor, *How Fair Is Safe Enough? The Cultural Approach to Societal Technology Choice*, 7 RISK ANALYSIS 3 (1987) (examining the role of fairness in societal acceptance of a technology's safety, as well as the structures societies create to apportion risk and liability for undesired consequences of those technologies).

76. While the pendulum tends to swing back and forth between legal and legislative approaches to the problem, conventional wisdom since the late 19th century has generally favored some kind of liability scheme to account for health, safety, and environmental risks associated with new technologies. *See, e.g.*, Gary T. Schwartz, *The Character of Early American Tort Law*, 36 UCLA L. REV. 641 (1988) (tracing differing bases for judicial findings for liability as technologies—and Americans' use of those technologies—progressed). These processes almost always lag far behind the rapid advances of technology, however, as there are societal learning processes that often require significant amounts of time to understand the full implications of each new technology. *See, e.g.*, Mary L. Lyndon, *Tort Law and Technology*, 12 YALE J. REG. 137 (1995) (examining how judicial decisions on tort liability both helped, and were helped by, society's grappling with technology's implications).

77. This goal often gets packed into the technical shorthand term of "usability," which encompasses a wide array of design concepts, including understandability, learnability, efficiency, memorability, resilience in the face of errors, and user satisfaction. *See* Jakob Nielsen, *Usability 101: Introduction to Usability*, NIELSEN NORMAN GROUP (Jan. 3, 2012), https://perma.cc/DU3H-D3EH. Apple Computers' co-founder Steve Jobs built an entire company around the philosophy describing the ideal technologies as those that that "just work," that are "truly personal," and "delightful" to the user. *See* WALTER ISAACSON, STEVE JOBS 533, 563 (2011). For Jobs and many others in the technology community, this idea has taken on quasi-religious overtones, which could be partially traced back to Jobs use of Buddhism as the part of the inspiration for his idea of technology intuition. *Id.* at 35.

78. It should be noted that manufacturer interpretation of user resistance to security features can be more accurately traced to poor security design, which is too often tacked on as an afterthought to connected devices, resulting in poor security integration and implementation. *See, e.g.*, Paul Hyman, *Study Reveals Resistance to Strong Password Security*, COMM. ACM (Nov. 15, 2011), https://perma.cc/23BU-5NQL.

This desire to create technologies that can be so seamlessly integrated into our everyday lives, while understandable, has created an environment that makes it easier for manufacturers to hide poor security design from their users, which in turn has made it more difficult for our society to fully comprehend the potential impact of security vulnerabilities until it is too late.[79] A recent example of this phenomenon can be found in the massive distributed denial of service (DDOS) attack that affected a wide range of Internet services by hijacking millions of "invisible" connected devices such as printers, security cameras, and baby monitors to serve as the distributed platform for this attack.[80] Because these devices have become so widespread, and are increasingly part of our daily lives, we have a natural tendency to ignore them as ordinary everyday appliances, allowing manufacturers the opportunity to invisibly apportion the risks of poor security design to their users.

2. The Race to the Bottom

The market for connected technologies is quite large and continues to show year-over-year growth, but the profit margins on many of these devices have become razor thin as they rapidly become commodified.[81] Thus, in order to remain competitive in this tight—but potentially quite lucrative, given the projected vol-

79. The Silicon Valley approach to technology rewards those first to market, even when those products are of far lesser quality and reliability than later products to arrive. "It makes no sense to spend more on security than the original cost of the problem, just as it makes no sense to pay liability compensation for damage done when spending money on security is cheaper." Bruce Schneier, *Liability Changes Everything*, SCHNEIER ON SECURITY (Nov. 2003), https://perma.cc/45NR-3V9K.

80. *See What Is the Mirai Botnet?*, CLOUDFLARE, https://perma.cc/2Y3A-ELLK (archived Dec. 12, 2019); Robert Graham, Mirai and IoT Botnet Analysis, presented at RSA Conference 2017 (Feb. 13-17, 2017), https://perma.cc/9S5F-4D2J.

81. The Internet Data Corporation (IDC) estimates that the global market for connected devices could be upwards of $1.4 trillion by 2021, with verticals such as manufacturing, freight and shipping monitoring, and asset management leading the way. *See Worldwide Spending on the Internet of Things Forecast to Reach Nearly $1.4 Trillion in 2021, According to New IDC Spending Guide*, MARKETWATCH (Jun. 14, 2017), https://perma.cc/DJ6C-WX7A. While some premium products can still command healthy profit margins, manufacturers of cheaper commodity items are forced to minimize product costs to preserve what little profit there is in a competitive global market. *See* Bruce Schneier, *The Internet of Things Is Wildly Insecure—And Often Unpatchable*, WIRED (Jan. 6, 2014), https://perma.cc/5QXM-QC2C ("[Manufacturers] often have to send users new hardware because it's the only way to update a router or modem, and that can easily cost a year's worth of profit from that customer. This problem is only going to get worse, and more expensive. Paying the cost up front for better embedded systems is much cheaper than paying the costs of the resultant security disasters").

umes—market, manufacturers of connected devices must cut costs wherever possible. One of the first budget line items to go is often security due to its inherent costs and the in-house expertise required.[82]

A particularly troublesome result of this cost shaving to preserve the profitability of connected devices is the use of "white labeling" among manufacturers and distributers of connected technologies, where companies will buy or license connected devices that have been manufactured by other companies and rebrand them as their own, often adding some of their own software to the devices.[83] This phenomenon has created an entire ecosystem of connected devices that appear to come from different vendors, but often share portions of the same codebase.[84] If the original manufacturer of the connected device chose to cut corners on the security and reliability of their software, vulnerabilities in this code will be spread across a wide range of devices from many different technology vendors.[85] This unhealthy mix of increased complexity and manufacturers' decreased willingness to address the attendant security vulnerabilities pushes the cybersecurity risk onto their unsuspecting customers.

3. You Are Not the Customer

In the age of surveillance capitalism the perspective that describes the users of connected technologies as products rather than customers has become uncontroversial.[86] The enormous amounts of data we generate by using connected devices and other networked services can have significant value to the companies that collect it, a fact that has not been lost on marketers, who have long sought the

82. *See* Charles McLellan, *Cybersecurity in an IoT and Mobile World: The Key Trends*, ZDNET (Jun. 1, 2017), https://perma.cc/EGF8-5Q7Q ("[J]ust 30 percent of respondents said their organisation allocated sufficient budget to protect mobile and IoT apps."). Perhaps ironically, this phenomenon has been a boon for cybersecurity firms who are often tasked with post hoc security cleanup for devices and systems that have been poorly secured by their manufacturer. Gartner Research, for example, estimates that post hoc spending on connected technology security could reach $840 million by 2020. *See* Michelle Maisto, *IoT Security Will Reach $840 Million By 2020, Gartner Finds*, INFORMATIONWEEK (Apr. 25, 2016), https://perma.cc/W635-JZDR.

83. *See, e.g.*, Tom Pageler, *Is Everything Hackable In The Internet Of Things?*, FORBES (Apr. 5, 2017), https://perma.cc/GD47-84KQ.

84. *See* Chester Wisniewski, *Mirai, Mirai, On the Wall—Through the Looking Glass of the Attack on Dyn*, NAKED SECURITY BY SOPHOS (Oct. 24, 2016), https://perma.cc/JF4C-K3ML ("The trouble with the hardware that has been hijacked for Mirai is that the devices are 'white label' goods, produced by an unbranded manufacturer for third-party companies").

85. *Id.*

86. *See, e.g.*, Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 30 (2015). This idea predates connected technologies, and has been used to describe the advertising model of television, as well. *See* KunstSpektrum, *Richard Serra "Television Delivers People" (1973)*, YOUTUBE (Feb. 2, 2011), https://perma.cc/W7K9-C733.

kinds of detail that can be found in our digital "exhaust."[87] Indeed, as we incorporate connected technologies into more and more facets of our daily lives, we are inevitably creating large amounts of detailed data that can reveal a surprising amount about our public and private lives, and technology manufacturers and service providers have focused on this fact as a potential revenue source.[88] Regardless of whether legitimate uses of user data exist—a question beyond the scope of this Article—this quest for more, and more detailed, user data creates a significant risk of moral hazard.

A recent example of this risk can be found in the use of in-home voice assistant technologies such as Amazon's Echo and Google's Home.[89] These are connected devices equipped with microphones that are designed to be placed throughout the user's home, giving the user the ability to interact with the device through voice conversations and instruct it to perform tasks like home automation control, Internet queries, and retail shopping.[90] As manufacturers rush to provide devices for this relatively new market, however, security vulnerabilities are bound to appear. In Google's case, for example, its Home product was recently found to contain a flaw that made some of its devices record all user conversations rather than only those the user designated through the voice or physical interface of the device.[91] Google quickly reacted to this vulnerability by publishing a software update, but what happens when a future vulnerability is exploited before Google identifies it—and what happens when companies without the resources of a Google start manufacturing such devices? If home automation assistants become commodities—with the attendant small profit margins—manufacturers competing primarily on price will likely jettison security spending. And even if home automation assistants do not become commodities, vulnerabilities appearing in today's top products suggest even current levels of security spending may not be enough.

4. Innovation Over Maintenance

The uniquely American concept of technology advancement has long given much more credence to innovation over maintenance, a philosophy that naturally carried over to Silicon Valley (both geographically and metaphorically) since the

87. *See generally* DALE NEEF, DIGITAL EXHAUST: WHAT EVERYONE SHOULD KNOW ABOUT BIG DATA, DIGITIZATION, AND DIGITALLY DRIVEN INNOVATION (2015).

88. *Id.*

89. *See Alexa Connected Devices: Connect Your Devices to Alexa to Reach and Delight More Customers*, AMAZON ALEXA, https://perma.cc/D8HR-Z85U (archived Dec. 12, 2019); *Google Nest and Google Home Device Specifications*, GOOGLE NEST HELP, https://perma.cc/LK3L-JZ3V (archived Dec. 12, 2019) (descriptions of Amazon's and Google's home automation technologies).

90. *Alexa Connected Devices*, *supra* note 89; *Google Nest Specifications*, *supra* note 89.

91. *See* Dieter Bohn, *Google's Home Mini Needed a Software Patch to Stop Some of Them From Recording Everything*, THE VERGE (Oct. 10, 2017), https://perma.cc/65V3-ZMXF.

days of the transistor.[92] This concept has become so integrated into our culture that we often equate the terms "technology" and "innovation" in everyday speech, and often presume that innovation is intrinsically superior to the more mundane tasks of analysis, maintenance, and repair. In fact, this idea has since been expanded in technology culture to include a certain reverence for disruption as a positive attribute for technological advancement.[93] This outlook has been of critical importance to the growth of the technology industry, and these philosophies have been widely adopted across nations and industries seeking to take part in the increasingly lucrative technology market.[94]

But the flip side of this approach has been the general neglect for a technology culture that values maintenance as a useful property. In the realm of connected technology, this means the regular review and upkeep of the software that sits on the millions of devices in use around the world.[95] We have already begun to see the long-term effects of this practice, with millions of connected devices being subverted annually.[96] This approach is a clear imbalance of risk based on information asymmetries between manufacturer and user, where manufacturers are pushing the costs of poorly maintained and secured devices onto the users.

Examples of the effects of Silicon Valley's storied reverence for innovation above all else can be found in the recent failings of Facebook and Uber.[97] Both of these companies have been widely lauded for their explosive growth over the past few years, with much of the credit for their successes attributed to Facebook founder Mark Zuckerberg's famous mantra, "move fast and break things."[98] This philosophy generally reflects the overall innovation-over-maintenance approach, where a company's agility—their ability to rapidly move from idea to prototype to product, often with little to no difference between these phases—was seen as the critical component for success, even if it meant shipping flawed hardware and software to their customers.[99]

One of the more significant problems with this approach is the increased risk associated with a company's inability (or unwillingness) to seriously consider the

92. *See* CHRISTOPHE LÉCUYER, MAKING SILICON VALLEY: INNOVATION AND THE GROWTH OF HIGH TECH, 1930-1970 (2006).

93. *See* Andreessen, *supra* note 56.

94. *Id.*

95. *See* Andy Oram, *The Alarming State of Secure Coding Neglect*, O'REILLY MEDIA (May 2, 2017), https://perma.cc/Z8BA-5WQA.

96. *See* Schneier, *supra* note 81.

97. These are only two particularly well-known examples of this problem, and I do not mean to imply that they occupy the entire universe of the innovation-over-maintenance effect.

98. In 2009, when asked about the source of Facebook's success, Zuckerberg was quoted as saying, "Move fast and break things. Unless you are breaking stuff, you are not moving fast enough." Henry Blodget, *Mark Zuckerberg on Innovation*, BUSINESS INSIDER (Oct. 1, 2009), https://perma.cc/ZX6Q-7TG3.

99. *See generally* JONATHAN TAPLIN, MOVE FAST AND BREAK THINGS: HOW FACEBOOK, GOOGLE, AND AMAZON CORNERED CULTURE AND UNDERMINED DEMOCRACY (2017).

negative consequences of their design decisions in the race to innovate. For example, in March 2018, multiple news outlets revealed documents showing that a UK-based data profiling company, Cambridge Analytica, improperly harvested the private information of as many as 87 million Facebook users, and used those data in their efforts on behalf of clients to influence elections and other political processes around the world.[100] The revelations drew immediate criticism from lawmakers in the United States and United Kingdom, who questioned Facebook's design and policy choices, and raised the idea that companies like Facebook could largely avoid the costs of these risks because the negative effects were largely paid for by their users.[101] The Facebook-Cambridge Analytica incidents revealed the problem of moral hazard and that Facebook had succumbed to it, prompting one British M.P. to declare Facebook a "morality-free zone."[102] Lawmakers on both sides of the Atlantic raised the possibility of increased regulation to combat this problem—and Zuckerberg appeared open to this possibility—but these calls lacked the sort of specificity required for real debate on the issue.[103]

Similarly, Uber, the ride-sharing company once called the "world's most valuable startup," maintained an innovation-over-maintenance philosophy that was, if anything, more remorseless than the Silicon Valley norm.[104] Uber's development of self-driving car technologies put it in direct competition with Google's automation research lab, Waymo, which filed a lawsuit in 2017 accusing Uber of stealing 9.7GB worth of trade secrets through a former Google employee.[105] Documents produced by Uber during discovery revealed a company that directly urged its employees to always move faster by ridding themselves of "the combination of risk aversion and lack of urgency."[106] This operating philosophy was encouraged at Uber from the top down, starting with then-CEO Travis Kalanick,

100. *See* Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://perma.cc/M327-YPAE; Craig Timberg et al., *Facebook: 'Malicious Actors' Used Its Tools To Discover Identities and Collect Data on a Massive Global Scale*, WASH. POST (Apr. 4, 2018), https://perma.cc/ZVS3-PLWC; Cecilia Kang & Sheera Frenkel, *Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users*, N.Y. TIMES (Apr. 4, 2018), https://perma.cc/22YW-8735.

101. *See* Jessi Hempel, *Congress Is Unearthing Facebook's Terrible Power*, WIRED (Apr. 11, 2018), https://perma.cc/7ZR7-5LQD.

102. *See* Jim Waterson, *'Facebook Is a Morality-Free Zone': Tech Chief Lambasted by MP*, THE GUARDIAN (Apr. 26, 2018), https://perma.cc/TQ4G-RNLZ.

103. *See* David Pierson, *Facebook's Mark Zuckerberg Says Cambridge Analytica Got His Personal Data Too*, LOS ANGELES TIMES (Apr. 11, 2018), https://perma.cc/8VP7-BBHR.

104. *See* Eric Newcomer & Brad Stone, *The Fall of Travis Kalanick Was a Lot Weirder and Darker Than You Thought*, BLOOMBERG BUSINESSWEEK (Jan. 18, 2018), https://perma.cc/DB3V-FGA4.

105. *See* Cyrus Farivar, *Waymo and Uber End Trial with Sudden $244 Million Settlement*, ARS TECHNICA (Feb. 9, 2018), https://perma.cc/69WB-H2M4; Waymo LLC v. Uber Tech., Inc., 319 F.R.D. 284 (N.D. Cal. 2017).

106. *See* Sarah Jeong, *Uber's Former Head of Self-Driving Cars Put Safety Second*, THE VERGE (Mar. 20, 2018), https://perma.cc/UA6J-7FVJ.

who had been building an unhealthy reputation for ignoring social and cultural norms, as well as actual laws.[107]

The parties in *Waymo v. Uber* unexpectedly settled their trade secret lawsuit in February 2018, but the questions regarding their innovation-over-maintenance approach raised by the documents that were revealed in that case deserve even more scrutiny than the intellectual property claims in the original complaint.[108] A particularly sobering example of the costs accruable to the risks associated with such an approach is the death of a Tempe, Arizona woman after she was hit by an autonomous Uber vehicle in March 2018.[109] Even after a man died in a Tesla-designed automated vehicle in May 2016, the head of Uber's automation project was quoted as telling his engineers to be even more aggressive in their pace, lamenting that he was "pissed [Uber] didn't have the first [automated vehicle] death."[110]

5. The Complexity-Vulnerability Relationship

The software behind connected technologies is, by its very nature, complex. Further, this complexity has a tendency to grow as a product matures, since new versions of these products almost always add, rather than subtract, features, which requires more software code, which adds to the overall complexity of the product.[111] This complexity creep makes it more difficult for developers to fully understand the detailed workings of this code, especially as codebases for software products are inherited by developers who were not part of the original team of designers and programmers.[112] There is a correlation between software developers' ability to understand their software and their ability to identify and address potential security vulnerabilities in this code.[113]

---

107. *See id.*

108. *See* Farivar, *supra* note 105.

109. *See* Andrew J. Hawkins, *Uber Halts Self-Driving Tests After Pedestrian Killed in Arizona*, THE VERGE (Mar. 19, 2018), https://perma.cc/SQP4-RYH7.

110. It should be noted that Anthony Levandowski, the executive quoted, has denied saying this. *See* Reeves Wiedeman, *Is Uber Evil, or Just Doomed?*, N.Y. MAG. (May 29, 2017), https://perma.cc/YJ5Q-7XUE.

111. *See* HORST ZUSE, SOFTWARE COMPLEXITY: MEASURES AND METHODS (1991).

112. This is often referred to in software circles as the "software Peter principle," which describes a project that has become so complex that its own developers cannot maintain it. *See* STEVE MCCONNELL, CODE COMPLETE: A PRACTICAL HANDBOOK OF SOFTWARE CONSTRUCTION (1993).

113. It is important to point out that there is significant disagreement among computer science scholars as to the correlation between software security and complexity. For example, a study that examined software based on a number of well-known complexity metrics found that the correlation between complexity and security was weaker than had been previously asserted. *See* Yonghee Shin & Laurie Williams, *Is Complexity Really the Enemy of Software Security?*, PROC. 4TH ACM WORKSHOP ON QUALITY OF PROTECTION 47 (2008). The point I wish to emphasize here is not the general correlation, but the problems that arise when developers fail to understand their own code.

The complexity of connected devices is not, in itself, the root of the security problem; rather, it is our limited ability as humans to completely understand the inner workings and potential interactions between highly complex systems that gives rise to security vulnerabilities. This problem is especially pervasive in the realm of partially commoditized connected devices, where manufacturers compete primarily on price but also on features—a combination that leads to increasingly complex codebases and few resources to assess and address the potential security vulnerabilities of that code.[114]

In addition, because connected devices are designed to interact with users or other devices through their external interfaces, these connection points often serve as vectors through which vulnerabilities may be exploited, especially as these interfaces themselves become more complex.[115] These "seams" between devices are especially vulnerable when the connected devices are designed—explicitly or implicitly—to deal with unstructured data, or use incorrect implementations of security protocols (which can be quite complex pieces of software by themselves).[116]

6. The Interconnectedness Problem

As implied by the name, connected devices operate under the principle that they maintain some external interface through which they send and receive data. This in itself creates a new set of problems that can grow as an exponential function of the number of devices accessible on a given network.[117] That is, connected devices can be used as vectors for the widespread exploitation of security vulnerabilities, where access to a vulnerable node acts as a platform from which to launch subsequent attacks on other connected devices. This can take the form of using a device vulnerability to replicate exploitative code across like devices, of using a device vulnerability as a gateway to bypass perimeter security mechanisms like firewalls, or of using a device as a vulnerable host from which to launch attacks on different kinds of devices. If done well, each of these exploitative categories of technique can often take place without the user of the originally exploited

114. *See, e.g.*, Russ Banham, *IoT Complexity*, RISK MGMT. (Aug. 1, 2016), https://perma.cc/2QCR-DFHS.

115. *See, e.g.*, Tom Gillis, *Complexity Is the Enemy of Security*, NETWORK WORLD (Aug. 8, 2016), https://perma.cc/87CJ-FSFL.

116. *See, e.g.*, Michael Kassner, *No Surprise, IoT Devices Are Insecure*, TECHREPUBLIC (Aug. 11, 2014), https://perma.cc/5VPK-H9PQ.

117. The network theoretic reasons for this exponential growth are based on the degree distribution $P(k)$ of a network, which is the probability distribution of the numbers of connections each node on that network has to other nodes. $P(k)$ is defined to be the fraction of vertices in the network with degree k. If n_k of these vertices have degree k, then $P(k) = n_k/n$. For networks like the Internet (and its sub-network, the Web), the degree distributions tend to follow a power law, where $P(k) = k^{-(\alpha-1)}$, for some constant exponent α. *See* Mark E.J. Newman, *The Structure and Function of Complex Networks*, 45 SIAM REV. 167, 185-86 (2003).

device knowing a thing about that device's role in the network-enabled spread of these attacks.

An increasingly common form of this phenomenon is the use of connected devices to create a vast army of "bots" by surreptitiously putting rogue software on these devices, which sits dormant until the malicious code's author activates it to flood other targeted devices with network traffic, overloading them and rendering them useless. These are known as distributed denial-of-service, or DDOS, attacks. A recent example of this can be seen in the late-2016 Mirai botnet attack, named for the software that was used to remotely take over infected devices.[118] The Mirai software created its botnet by exploiting vulnerabilities found in connected devices like webcams, which many users do not even think of in the same way they consider other connected devices like smartphones and computers.[119] Vulnerabilities on such devices often go unpatched, either because the manufacturer elects not to spend money on security (see Part III.A.1 above), or because users do not apply available security patches.[120] The Mirai botnet was used to take down popular sites such as KrebsOnSecurity, a security analyst and frequent critic of hackers, the French web hosting company OVH, the Dyn Domain Name System provider, and possibly even the entire country of Liberia.[121] These attacks, which may not affect any connected device's individual end-user, show that technology makers and service providers face not only moral hazard with respect to individual users, but to society in general: Technology makers and service providers can impose risks on third parties who are unlikely or even unable to notice and react in a way that reduces the profits the technology makers enjoy by selling vulnerable devices.

B. Technological Trust and the Usual Solutions

Because of the unique characteristics of cybersecurity's moral hazard problem, the usual solutions are insufficient by themselves. Historically, resolutions of moral hazards arising from information imbalances between manufacturer and consumer have relied upon contracts or torts law to rebalance incentives, but for reasons that will be discussed in the next Part, these approaches fall short when it comes to resolving cybersecurity moral hazard.[122]

For any new technology to gain acceptance within society, a critical mass of consumer trust must be built and maintained, based not only on the perceived

118. *See* John Biggs, *Hackers Release Source Code for a Powerful DDoS App Called Mirai*, TECHCRUNCH (Oct. 10, 2016), https://perma.cc/KV68-E5KB.

119. *See* Lily Hay Newman, *The Botnet That Broke the Internet Isn't Going Away*, WIRED (Feb. 9, 2016), https://perma.cc/N8B6-59DL .

120. *See* Brian Krebs, *Who Makes the IoT Things Under Attack?*, KREBS ON SECURITY (Oct. 3, 2016), https://perma.cc/X2QG-UXJT.

121. *See* Brian Krebs, *Did the Mirai Botnet Really Take Liberia Offline?*, KREBS ON SECURITY (Nov. 16, 2016), https://perma.cc/6BRJ-UZGW; Newman, *supra* note 119.

122. *See infra* Part IV.

usefulness of the technology, but also on the safety and reliability of the product.[123] Technological advances have provided the bases for societal change in countless ways, not only through the increased abilities these technologies have given us, but also through the myriad ways in which we relate to one another through these technologies.[124] Because the products of new technologies have been of such central importance to human advancement, methods of resolving manufacturer moral hazards take on a significance that goes far beyond the relationship between the user and the product.[125] Rather, these approaches are meant to rebalance the relationships between user and manufacturer, and in a larger moral sense, the relationships within societies.[126]

The typical approaches to this dilemma, however, fail to account for the unique problems posed by cybersecurity. These unique characteristics amplify the information asymmetries between manufacturer and user and mask the true extent of these asymmetries behind a black box. Connected devices, in other words, depend on—and force—an extreme level of user trust, or even blind faith. To make things worse, manufacturers have begun to intentionally conceal functionality from users not for reasons of usability, but rather to limit the user's ability to judge for herself the risks inherent in the product.[127]

IV. ADDRESSING CYBERSECURITY'S MORAL HAZARD

Because the unique characteristics of connected technologies make historical approaches to resolving associated cybersecurity moral hazard less effective, it is necessary to adjust our thinking about this special case. In this Part, I lay out five recommended actions that form the basis for a comprehensive approach to this problem. Each of these actions can be useful by themselves, of course, but I posit

123. *See* Paul A. Pavlou, *Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model*, 59 INT'L. J. ELECTRONIC COMM. 69 (2003).

124. *See* George Priest, *A Theory of the Consumer Product Warranty*, 90 YALE L.J. 1297 (1981); Owen, *supra* note 51.

125. *See* Priest, *supra* note 51.

126. The moral and ethical considerations of manufacturer liability are not often discussed in current literature, but do provide the basis of modern tort theory, especially products liability. That is, a manufacturer's liability for their products is based upon the foundational moral question of how people (and organizations) should treat one another in a just society, and thus seeks to answer questions about the moral responsibility for injury due to product failures. *See, e.g.*, David G. Owen, *Moral Foundations of Products Liability Law: Toward First Principles*, 68 NOTRE DAME L. REV. 427 (1993); Priest, *supra* note 51.

127. This is, of course, a matter of some controversy, as manufacturers will argue that their concealment of certain functionality is done not to deceive the user, but instead is done for reasons of ease-of-use, trade secrecy, privacy, or other legitimate purposes. Either way, this black box approach has become increasingly the norm in connected device design, and users often have no choice but to trust in the safety and reliability of these devices. *See, e.g.*, PASQUALE, *supra* note 2.

that any long-term solution to the problem of cybersecurity moral hazard requires at least some measure of each of these categories.

A. Create or Enhance Cybersecurity Incentives

Solutions to moral hazard problems often seek to counter the inherent issues with information asymmetries by creating or adjusting incentives designed to adjust for risk imbalances.[128] While this approach has successfully been applied to resolve other instances of moral hazard, it has been insufficient in addressing the unique problems inherent to the security of connected technologies for both natural and artificial reasons. As discussed above in Part III, there are a number of inescapable properties of connected technologies that make these solutions to information imbalances untenable.[129] Further, the liability and regulatory regimes that have historically been the basis for manufacturer incentives for most other products and industries have been rendered less useful with respect to software and connected devices.[130]

Products liability for security vulnerability in connected devices falls into gray areas for a number of reasons, some based on prior doctrine, and others that have been molded around software and related technologies. The doctrine of economic loss, for example, prohibits recovery in tort for purely economic losses without personal injury or damage to property.[131] This has historically covered most damages stemming from security flaws in connected devices, which forces most disputes between user and manufacturer to sound in contract.[132] The principles behind design defects have also played a role in making this approach less effective, since the complexity of software design often makes it difficult for a user to show that a particular connected device's design is, indeed, defective.[133]

---

128. *See supra* Part II.C.

129. *See supra* Part III.

130. *See* Frances Zollers et al., *No More Soft Landings for Software: Liability for Defects in an Industry That Has Come of Age*, 21 SANTA CLARA HIGH TECH. L.J. 745 (2005); *see also* Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425 (2008); Michael Rustad & Lori Eisenschmidt, *The Commercial Law of Internet Security*, 10 HIGH TECH. L. REV. 213 (1995).

131. *See* Vincent R. Johnson, *The Boundary-Line Function of the Economic Loss Rule*, 66 WASH. & LEE L. REV. 523 (2009); David Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935 (2016).

132. The economic loss doctrine has been a point of disagreement between courts and scholars, and the Third Restatement of Torts was meant to address at least some of these concerns. RESTATEMENT (THIRD) OF TORTS: LIAB. ECON. HARM (AM. LAW INST., Tentative Draft No. 1, 2012).

133. *See* Jill Wieber Lens, *Warning: A Post-Sale Duty To Warn Targets Small Manufacturers*, 2014 UTAH L. REV. 1013 (2014).

But the problem of cybersecurity moral hazard is just the sort of manufacturer-user conflict that products liability was created to solve.[134] Manufacturers, rather than users, are in the better position to mitigate damages, especially when those manufacturers force a negative externality onto their customers.[135] The long-term risks of continuing down the reduced liability path for manufacturers will only lead to greater damage to individuals, institutions, and governments.

The area where the incentivization of technology manufacturers will likely bear the most fruit is in the rethinking of the innovation-over-maintenance culture that pervades the technological industry. Because there is often little financial incentive, many technology companies underinvest in the security of their products.[136] Technology manufacturers are incentivized, however, by the profits they turn by releasing new or updated products, so they invest heavily on the innovation side through, for example, offering very high salaries (and associated prestige) for software developers, while underinvesting in security design and engineering.[137] Simply put, the costs of a security vulnerability in a product often seem miniscule in comparison to the profits realized by the early release of that product. But this arithmetic is incorrect—there are costs associated with these security vulnerabilities, but they are often borne mainly by consumers and third parties.

It is therefore important to provide new motivations for technology companies to steer more resources toward security design and product maintenance. These motivations should come in the form of legal and economic incentives, including carefully planned federal and state regulation and reconsideration of liability in tort or contract. The current state of cybersecurity regulation is often described as a "patchwork" of laws at federal and state levels that lack the sort of coordination and coherence necessary to effectively promote the security of our connected technologies. In addition, current tort and contract law has similarly yielded a largely ineffective mixed bag of results—and confused incentives—for both technology manufacturers and consumers.[138]

134. Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 U. CHI. PRESS J. 221 (2006).

135. *Id.*

136. *See, e.g.*, Erik Sherman, *The Reason Companies Don't Fix Cybersecurity*, CBS NEWS (Mar. 12, 2015), https://perma.cc/7698-C8W5.

137. *See, e.g.*, Alex Blau, *The Behavioral Economics of Why Executives Underinvest in Cybersecurity*, HARV. BUS. REV. (Jun. 7, 2017), https://perma.cc/853P-LRUE.

138. *See, e.g.*, Geistfeld, *supra* note 51; Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, 50 U. MICH. J.L. REFORM 913 (2017).

From a federal perspective, the Federal Trade Commission (FTC) has emerged as the primary enforcer of cybersecurity obligations, drawing its authority under Section 5(a) of the Federal Trade Commission Act.[139] Enforcement actions through the FTC generally begin with an investigation of a company's cybersecurity practices; depending on the results of that investigation, the FTC may then issue a draft complaint containing a list of alleged violations of Section 5 of the FTC Act. Most often, companies will enter into some kind of settlement with the FTC, resulting in a consent decree. If, however, a settlement cannot be reached, the FTC may seek enforcement through its own administrative capacity under Section 5(b) of the FTC Act (via injunctive relief), or in federal court under Section 13(b).[140]

While the number of cybersecurity enforcement cases brought by the FTC continues to grow, there are signs that these actions alone are not enough to provide the incentives necessary for companies to avoid cybersecurity moral hazard.[141] For example, in the past ten years, only about a quarter of FTC settlements and judgments have resulted in full compliance or restitution, due in large part to defiance of terms by companies, insufficient funds, and the concealment of assets by companies in violation of Section 5.[142] This statistic is indicative of two factors at work. First, there are a significant number of companies that—even after investigations have shown substantial violations of their cybersecurity obligations to their customers—are willing to evade compliance or to spend time and resources fighting to show they are already in compliance with settlements rather than address the underlying problems with their cybersecurity policies and procedures. Second, while federal case law has generally been very favorable to the FTC in its pursuit of relief under Section 13(b) of the FTC Act, the agency often has difficulties enforcing resulting orders, since courts require the FTC to prove by clear and convincing evidence that a company has expressly violated some part

139. *See generally* 15 U.S.C. § 45(a) (2012). The FTC has established its data security enforcement standards through its authority to prohibit "unfair or deceptive acts or practices in or affecting commerce" under § 5 of the FTC Act. *Id.* The FTC's claimed basis for this authority was directly challenged in 2014 by Wyndham Worldwide after the FTC alleged that Wyndham had violated the FTC Act through their "failure to maintain reasonable and appropriate data security for consumers' sensitive personal information." FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015). The District Court held—and the Third Circuit affirmed—that the FTC does have the authority to regulate "unfair" cybersecurity failures under § 5 of the FTC Act. *Id.*

140. 15 U.S.C. § 53(b) (2012). It is worth noting that the FTC can only obtain monetary damages through this section, which authorizes the FTC to seek not only injunctive relief, but may also freeze corporate assets, disgorge profits, and seek monetary or other restitution. *Id.*

141. From 2002 through 2018, the FTC brought 65 cases against companies engaging in unfair or deceptive practices involving the inadequate protection of consumers' personal data. FEDERAL TRADE COMMISSION, PRIVACY & DATA SECURITY UPDATE 5 (2018).

142. *See* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016).

of an order, and violations involving the privacy and security of consumer data are quite slippery to define, let alone prove, to the satisfaction of courts.[143]

An apt example of the latter effect may be found in the years-long struggle between the FTC and LabMD, a medical diagnostics company who was accused by the FTC of "engag[ing] in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks."[144]

Following a trial before an administrative law judge, the FTC's complaint was dismissed based on the grounds that the FTC had failed to prove that LabMD's failure to employ reasonable cybersecurity policies and procedures either caused or was likely to cause harm to consumers.[145] The FTC appealed this decision, and found that LabMD's cybersecurity practices were unfair and were likely to cause substantial consumer injury, issuing a cease and desist order requiring LabMD to "establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers."[146] LabMD appealed this decision.[147]

On June 6, 2018, the Eleventh Circuit vacated the FTC's enforcement order against LabMD, holding that the order was insufficiently specific, and therefore unenforceable, because it "does not instruct LabMD to stop committing a specific act or practice," but rather "commands LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness."[148] The court pointed to a likely battle between cybersecurity experts, where the FTC would likely call an expert to testify that LabMD's security practices were not reasonable, while LabMD would likely provide its own expert who would disagree.

State agencies are also taking an increased interest in cybersecurity. Through California's unfair competition law ("UCL"), for example, any "unlawful, unfair,

143. *Id.*

144. *In re* LabMD, Inc., 2015 WL 7575033 (F.T.C. Nov. 13, 2015) (initial decision).

145. *Id.*

146. *See In re* LabMD, Inc., 2016 WL 4128215 at *1, 33 (F.T.C. July 28, 2016) (final order).

147. LabMD, Inc. v. FTC, 894 F.3d 1221, 1227 (11th Cir. 2018).

148. *Id.* at 1221, 1236. It is worth noting here that LabMD ceased operations in 2014, claiming that their business could not bear the costs imposed by the FTC investigation and subsequent litigation. *Id.* at 1224. An interesting thought experiment might be constructed by an analysis of the costs associated with fighting the original FTC investigation versus investing in the analysis and implementation of industry standard cybersecurity practices. For example, among the cybersecurity issues found in the original FTC investigation were multiple basic violations of industry standards, including the multiple employees using the same login credentials, an absence of any kind of file integrity monitoring or network intrusion detection system, and the installation of P2P file sharing software on a department manager's computer, resulting in the wide distribution of multiple documents subject to federal privacy laws. *Id.* The fact that LabMD resisted the implementation of basic cybersecurity standards and elected instead to spend time and money fighting the FTC points toward a reluctance to come to terms with cybersecurity moral hazard, at least in this instance.

or fraudulent business act or practice" is prohibited.[149] Under this law, companies that store, transmit, or use Californians' consumer information may attract the attention of the Attorney General's office for violating the UCL through poor cybersecurity practices. For example, in 2014, the California Attorney General filed a complaint in state court against Kaiser Foundation Health Plan, alleging that Kaiser had violated the UCL by publicly posting the Social Security numbers of more than 20,000 Californians.[150] The court rendered judgment in favor of the State, ordering Kaiser to develop additional cybersecurity training and policies, conduct an audit of its employees' access to protected information, and pay a fine plus attorney's fees.[151] California has also been a leader in privacy-related legislation, most recently enacting the California Consumer Privacy Act (CCPA), enacted in 2018.[152] With other states moving to create their own privacy laws, many of which providing more rigorous approaches to data security than those available at the federal level, states now appear to be a leading vector for cybersecurity incentives.[153]

But despite these existing regulatory efforts, technology companies often choose to shave their development costs by reducing or eliminating resources necessary to support secure software development.[154] These priorities are passed down from management to staff, both through general development cultures within the company and internal financial incentives presented to individual contributors.[155] Further, far too many developers within these technology companies lack the security skills necessary to identify and mitigate software vulnerabilities in their code, due in large part to the fact that developers with security education and experience tend to be more expensive, and the time needed to perform adequate security audits and fix vulnerabilities adds costs to projects, costs that the companies themselves are not incentivized to bear.[156]

149. CAL. BUS. & PROF. CODE §§ 17200-01 (West 2019).

150. Complaint, California v. Kaiser Found. Health Plan, Inc., No. RG14711370 (Cal. Sup. Ct. Jan. 24, 2014), https://perma.cc/8G2N-MB99.

151. Stipulation for Entry of Final Judgment, California v. Kaiser Found. Health Plan, Inc., No. RG14711370, 2014 BL 379280 (Cal. Sup. Ct. Jan. 24, 2014), https://perma.cc/5UKH-CDUF.

152. California Consumer Privacy Act, 1798 CAL. CIV. CODE §§ 100-99 (West 2018).

153. *See* Cynthia Brumfield, *11 New State Privacy and Security Laws Explained: Is Your Business Ready?*, CSO ONLINE (Aug. 8, 2019), https://perma.cc/Q4UM-JBD9; Cameron F. Kerry, *A Federal Privacy Law Could Do Better Than California's*, BROOKINGS (Apr. 29, 2019), https://perma.cc/VXQ5-Q3R7.

154. *See supra* Parts III.A.2 and III.A.4.

155. In a recent survey, 56% of developers, operations, and security professionals reported that, in their organizations, developers are not generally evaluated based on security vulnerabilities in products they help build. *See* GITLAB, 2019 GLOBAL DEVELOPER REPORT: DEVSECOPS 15 (2019), https://perma.cc/CG4B-ZLK7.

156. *See supra* Parts III.A.2 and III.A.4.

B. Revamp the Software Curriculum

In order for manufacturers of connected devices to build in a reasonable amount of security—and follow that up with product support and security updates—they must employ designers, developers, and engineers who understand the basic tenets of software security design, much as bridge construction companies must employ architects and engineers who understand the basics of materials science, physics, and structural design.[157] A critical difference between these two fields (despite the somewhat misleading use of "software engineer" in the technology industry) lies in the fact that, unlike true engineering disciplines, such as mechanical engineering and aeronautical engineering, software development lacks the regulations, certification requirements, apprenticeship programs, and continuing education requirements of the former disciplines.[158] And while it is perhaps unreasonable to expect the software industry to immediately adopt the rigorous standards that apply to engineering disciplines, it is important to start moving in that direction, which requires a modification of the way we think about training software developers and designers. The structural integrity of the technologies that occupy our lives, from the trivial to the essential, is too often designed and coded by people with no training in software security principles. A significant part of the solution to this problem lies in the education of our software designers and engineers.[159]

Part of this educational problem lies in the history of the computer industry. In the early days of computer programming, computers were big, rare, and required a high degree of skill to use or program.[160] When personal computers began showing up in people's homes in the late 1970s and early 1980s, anyone who could afford one could learn to program one.[161] These early steps toward ubiquitous computing created a revolution, allowing amateur hobbyists the opportunity to learn to program computers on their own time.[162] Interest in university computer science programs—a relatively new field in academia, one that got its start in the mathematics departments of many institutions—also grew, as employment opportunities in software and related technologies rapidly expanded.[163]

---

157. *See* Ian Bogost, *Programmers: Stop Calling Yourselves Engineers*, THE ATLANTIC (Nov. 5, 2015), https://perma.cc/XS2Q-QYXS.

158. *Id.*

159. *See, e.g.*, *Infographic: A Lack of Software Security Training Puts You at Risk*, SOFTWARE INTEGRITY BLOG (Jan. 22, 2018), https://perma.cc/L4WC-XLPC; Warwick Ashford, *Developers Lack Skills Needed for Secure DevOps, Survey Shows*, COMPUTER WEEKLY (Aug. 17, 2017), https://perma.cc/H8VR-DVMB; Steve Morgan, *Is Poor Software Development the Biggest Cyber Threat?*, CSO ONLINE (Sept. 2, 2015), https://perma.cc/DJG4-TJY2.

160. Bogost, *supra* note 157.

161. *Id.*

162. *Id.*

163. *See* Gene I. Maeroff, *College Students Flock to Computer Science*, N.Y. TIMES (Jan. 14, 1985), https://perma.cc/G53W-BHP5.

But as software began to "eat the world," two problems emerged regarding the education of software developers. First, many university computer science programs fail to include sufficient security instruction in their required curricula, creating generations of computer programmers who often lack a full understanding of cybersecurity as part of their discipline.[164] Second, as an increasingly wide array of industries decided that they wanted to enter the connected technology market, they realized that they could often find more self-trained programmers. This is not to say, of course, that a university education is necessary to become a good software developer. Rather, these points show that there is very little in the way of a standard base curriculum in computer programming, and a wide range of programmers—from the university educated to the self-taught—lack a fundamental understanding of software security.

A common symptom of this problem can be found in the "copy and paste" culture that pervades software development in areas such as software security.[165] As forums for software developers began to proliferate on the internet in the early 1990s, this practice became more widespread, as it became relatively easy to find code that appeared to provide the functionality one might be seeking.[166] In 2017, a group of researchers analyzed the quality of the code that could be found on one of the most popular developer sites, and they found that many of the most referenced code samples on these sites contained security vulnerabilities, while, in some cases, the least referenced code samples contained the correct methods for resolving those vulnerabilities.[167]

While the public at large may still be unaware of some important details behind some of the more technical aspects of cybersecurity, most are aware of the general risks posed in a world where software and related technology have become ubiquitous in modern life, while lacking the details behind these generalized risks.[168] Yet in 2019, none of the top undergraduate computer science programs in the United States require any kind of rigorous course in computer or network

164. Yi Pan et al., *Integrating Security Education into a CS Curriculum*, 2016 ANNUAL ASEE CONF. & EXPOSITION (2016). *But see* Josephine Wolff, *Why Computer Science Programs Don't Require Cybersecurity Classes*, SLATE MAG. (Apr. 14, 2016), https://perma.cc/8CRF-YXMP.

165. "Copy and paste" programming is a term that refers to the common practice among software developers of finding software code that appears to provide the functionality they are looking for and copying it into their own code base. This technique is not considered bad practice if the programmer fully understands the code she is copying. Unfortunately, many programmers use this technique *because* they do not understand the code, and do not have the time or background to do so. *See, e.g.*, Zoltán Ádám Mann, *Three Public Enemies: Cut, Copy, and Paste*, 39 COMPUTER 31 (2006).

166. *Id.*

167. *See* Zeljka Zorz, *Secure Coding in Java: Bad Online Advice and Confusing APIs*, HELP NET SECURITY (Oct. 3, 2017), https://perma.cc/DWP7-UVNW.

168. *See infra* Part IV.C.

security as part of their core curriculum.[169] This curricular cybersecurity gap exists despite the fact that academics in the field have been calling for the inclusion of cybersecurity fundamentals in the computer science core curriculum for decades.[170]

The reasoning behind this historical institutional resistance is not unsound. Computer science academics generally agree that software developers and engineers should be better equipped to identify, analyze, and mitigate vulnerabilities in the technologies they are creating, but also note that four-year computer science curricula are already cramped for space. What course(s) would have to be dropped in exchange for security courses? Further, what should these security courses teach? Cybersecurity as a topic is far broader than any one course can encompass, so how can computer science departments possibly triage the subject to properly teach cybersecurity "basics"?[171]

These are valid points for consideration, but they must be weighed against the real-world results of such strategies. According to a July 2019 survey of security professionals, most believed that it was the job of the programmer to write secure code, but they also thought that fewer than one half of current developers had the skills or experience to reliably spot security vulnerabilities.[172] Further,

169. Based upon the top ten undergraduate computer engineering programs with graduate programs in engineering as compiled by U.S. News and World Report. *The Best Colleges for Computer Engineering*, US NEWS & WORLD REPORT, https://perma.cc/A8VW-NJVT (archived Oct. 3, 2019). The institutions surveyed were Carnegie Mellon University, MIT, Stanford University, University of California at Berkeley, Georgia Tech, University of Michigan, University of Illinois at Urbana-Champaign, Cornell University, University of Texas at Austin, and Purdue University-West Lafayette. For this purpose, I searched each program's undergraduate degree requirements for the 2019-2020 academic year. While computer or network security courses were offered as electives in each of these programs, none of them required such a course as part of the program's core curriculum. Some institutions did offer a computer security concentration or track within the larger computer science bachelor degree program, e.g., University of Texas and Purdue University. *See The University of Texas at Austin Computer Science: Concentrations*, UNIV. OF TEXAS AT AUSTIN, https://perma.cc/Z9C7-CJZ6 (archived Dec. 15, 2019); *Purdue University Department of Computer Science: Computer Science Degree Requirements*, PURDUE UNIV., https://perma.cc/G4AK-UQQE (archived Dec. 15, 2019).

170. *See, e.g.*, Cynthia Irvine et al., *Integrating Security into the Curriculum*, 84 ELECTRICAL ENGINEERING & COMPUTER SCI. 25 (1998); T. Andrew Yang, *Computer Security and Impact On Computer Science Education*, J. COMPUTING SCIENCES IN COLLEGES 233 (2001); Bradley Bogolea & Kay Wijekumar, *Information Security Curriculum Creation*, INFOSECCD CONF. (2004); Blair Taylor & Shiva Azadegan, *Moving Beyond Security Tracks*, PROC. 39TH ACM TECHNICAL SYMP. ON COMPUTER SCI. EDUC. 320 (2008); Michael E. Whitman & Herbert J. Mattord, *Designing and Teaching Information Security Curriculum*, PROC. 1ST ANNUAL CONF. ON INFO. SECURITY CURRICULUM DEV. 1 (2004).

171. *See* Wolff, *supra* note 164.

172. Suri Patel, *2019 Global Developer Report: DevSecOps Finds Security Roadblocks Divide Teams*, GITLAB (Jul. 15, 2019), https://perma.cc/9XA7-VQ9H; 2019 GLOBAL DEVELOPER REPORT, *supra* note 155.

half of the security professionals surveyed attested to difficulties in getting developers to make even basic cybersecurity a priority.[173] Even developers themselves recognize the problems a lack of cybersecurity foundations creates, pointing out that there is often little support within their respective organizations for providing the resources necessary for security training and development.[174] Thus, the skillset necessary for developers to write reasonably secure code is often limited to a relatively small group, most of whom are (or become) security professionals, removing themselves from the general software development talent pool. The resulting supply/demand cycle for software developers with a practical level of security knowledge raises the cost of product development, and unincentivized technology companies elect not to make that investment in the security of their products.[175] The heightened cybersecurity risks associated with those products are therefore left to be borne by the consumer.

Without the requirement of a base curriculum and continuing education opportunities and/or requirements for computer programming, even otherwise skilled developers will get caught in this trap, as time is so often a factor in the development of connected devices. Reforming the software development/computer science curriculum is therefore a necessary component to a sound resolution of cybersecurity's moral hazard. As discussed above in Part IV.C, this is not to suggest that programming mini-courses and coding boot camps are not useful tools in providing connected technology users a deeper understanding of the implications of their use of these devices. It does mean, however, that this level of understanding should not by itself be a sufficient education for software developers writing code that will be deployed on potentially millions of devices. This is, of course, anathema to the conventional wisdom that has pervaded the software industry since its earliest days.[176] As software has become a key part of our physical, economic, political, and social infrastructures, however, we need to revisit this conventional wisdom with an eye toward the long-term sustainability of this model.

---

173. Patel, *supra* note 172.

174. *Id.*

175. *See, e.g.*, *Why Some Companies Don't Invest in Cybersecurity*, COLUMBIA MAG., Fall 2015, https://perma.cc/3J98-JPNW; Adam Levin, *How Can 73 Percent of Companies Not Be Prepared for Hackers?*, INC. (Feb. 22, 2018), https://perma.cc/73FG-UUD5.

176. Formal education has long been rejected as a necessary component to software development with well-known examples of Bill Gates (who dropped out of Harvard to form Microsoft), Steve Jobs (who dropped out of Reed to later form Apple Computers), and Mark Zuckerberg (who dropped out of Harvard to form Facebook). *See* Paige Leskin, *These 23 Successful Tech Moguls Never Graduated College*, BUS. INSIDER (May 26, 2019), https://perma.cc/3MQU-WJRX.

C. Understand and Address the Technology Information Gap

It is axiomatic that connected technologies are, by their very nature, complex, and it is therefore unreasonable to expect an average user of these technologies to understand the details behind the inner workings of their connected devices. But the potential impact of a willingness to accept high levels of technology illiteracy—both on the part of manufacturers as well as users—is a significant enabling component of the information asymmetries that support cybersecurity moral hazard. For this reason, it is important that manufacturers make available additional information about the functionality (and risks) of their devices, as well as users educating themselves on technology basics.

A big part of the technology information gap between manufacturers and users is the long-known fact that a company that has an information advantage over its customers also has a foundation for increased profits from those customers.[177] This, coupled with our natural tendency toward automation bias, leads to the user's overconfidence and overreliance in the manufacturer's ability (or willingness) to ensure the security or reliability of their technologies.[178] Reasonably full disclosure on the part of the manufacturer, whether through regulatory, legislative, or private means, is a key factor in reducing these information gaps.

But users must also do their part to develop a level of technical literacy necessary to understand the risks disclosed by manufacturers. Without this basic grasp of connected technologies fundamentals, users often develop a sense of nihilism regarding cybersecurity, a factor that only exacerbates the information asymmetries that already exist between manufacturer and consumer.[179] Basic technological literacy does not require a computer science degree, of course; rather, it can be attained via basic technology courses in primary, secondary, and post-secondary education, as well as the use of a growing number of online courses on technology fundamentals.

We must also consider the constant tension between the security and usability of technologies. That is, the design of secure systems, with important features such as user authentication and access controls, creates additional hoops for the user of the technology to jump through, and even when the user is fully aware of the reasoning behind these security measures, their inclinations or outright necessity can cause them to ignore or create their own workarounds that can defeat the purpose of the security mechanisms. Take, for example, the task of securing

177. *See, e.g.*, G.N. Ismagilova et al., *Asymmetric Information and Consumer Demand*, 10 ASIAN SOC. SCI. (2014).

178. *See* Eugenio Alberdi et al., *Why Are People's Decisions Sometimes Worse with Computer Support?*, PROC. 28TH INT'L CONF. COMPUTER SAFETY, RELIABILITY, & SECURITY 18 (2009); Dietrich Manzey et al., *Misuse of Automated Aids in Process Control: Complacency, Automation Bias and Possible Training Interventions*, 50 PROC. HUM. FACTORS & ERGONOMICS SOC'Y ANN. MEETING 220 (2006); John D. Lee & Katrina A. See, *Trust in Automation: Designing for Appropriate Reliance*, 46 HUM. FACTORS 50 (2004).

179. *See, e.g.*, David Kravets, *Online Privacy Nihilism Runs Rampant in US, Survey Says*, ARS TECHNICA (Mar. 16, 2015), https://perma.cc/6PLD-DHWE.

medical devices in a hospital environment.[180] No one would argue that it is unnecessary to protect the patient health data displayed, analyzed, and stored on these devices, and in fact, the requirement to protect patient data is one of the comparatively few federal privacy laws currently on the books.[181] But studies have shown that, too often, the design of medical device security measures do not take into account the work environments of hospitals and medical clinics, which are driven by interruptions and nomadic, while the authentication and authorization interfaces on these devices are designed to accommodate users who work on single tasks for extended periods of time at one location.[182] The tension between these designs and the environmental demands of the healthcare workplace result in medical staff sharing passwords, manipulating login/logoff timeout mechanisms, and giving others without credentials access to restricted security levels.[183] It is more difficult and expensive to design security protocols that better suit user needs while, at the same time, providing the levels of cybersecurity required by regulation or policy. The risk associated with devices made by technology companies that elect not to take on these costs are thus borne by users and third parties.

D. Rethink Our Dated Technology Cost-Benefit Analysis

The cost-benefit analysis applied to design defect analysis considers a product "defective in design when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design."[184] A "reasonable alternative design," in turn, is defined in terms of costs and benefits: the costs of a (presumably) safer alternative design must be lower than the costs due to foreseeable injuries that would be prevented by sustaining the costs associated with the safer alternative design.[185] Applying this test, for example, if a feasible alternative design of a car's suspension system would cost less than the losses due to accidents that could be prevented by that part, that suspension design should be used.[186]

While this system has worked reasonably well for products in the past, it falls short when it comes to software and related technologies, mainly due to argu-

180. *See, e.g.*, Jakob E. Bardram, *The Trouble with Login: On Usability and Computer Security in Ubiquitous Computing*, 9 PERS. & UBIQUITOUS COMPUTING 357 (2005).

181. *See* 42 U.S.C. § 1320d-6(b); *see also* Andrew Burt, *States Are Leading the Way on Data Privacy*, THE HILL (Aug. 21, 2018), https://perma.cc/4KTC-ULVQ.

182. *See* Bardram, *supra* note 180, at 360.

183. *Id.*

184. RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2 (AM LAW INST. 1998).

185. Included in the costs of the safer alternative design are costs of manufacturing, loss of product usefulness, and any increase in costs due to different harms that may arise from the alternative design. *See* RESTATEMENT (THIRD) OF TORTS: LIAB. ECON. HARM, *supra* note 132, §2(b).

186. *See, e.g.*, Branham v. Ford Motor Co., 701 S.E.2d 5, 13-17 (S.C. 2010).

ments that this analysis should be adjusted to weigh heavily in favor of manufacturers out of fears that increased liability would stifle innovation.[187] This argument has lost much of its force as connected technologies continue to spread throughout most facets of contemporary society, where their failure can have widespread physical, economic, political, and social effects.[188] Other industries have fared quite well under a balanced regime that requires the manufacturer, as least-cost avoider, to bear its fair share of liability for flawed products. To continue with an artificially imbalanced analysis when it comes to connected technologies only serves to exacerbate the moral hazard problem.

On the regulatory side, the FTC has been increasingly reliant upon incumbent cost-benefit and economic analyses in their decision-making process.[189] The problem that often arises with this approach is the difficulty in attaching a precise dollar value to the harms caused by poor cybersecurity design and implementation by technology manufacturers. But the fact that these costs are uncertain should not be an impediment to all cybersecurity regulation. For some of these regulatory decisions, a new cost-benefit analysis will require ethical considerations and value judgments gained from privacy and data security experts and ethical review committees.

187. *See* Peter Alces, *W(h)ither Warranty: The B(l)oom of Products Liability Theory in Cases of Deficient Software Design*, 87 CALIF. L. REV. 269-304 (1999) (examining changes to UCC and products liability law that would address software defects); David W. Lannetti, *Toward a Revised Definition of "Product" Under the Restatement (Third) of Torts: Products Liability*, 55 BUS. LAWYER 799 (2000) (arguing for updates to products liability doctrine to keep up with technological changes); Lori A. Weber, *Bad Bytes: The Application of Strict Products Liability to Computer Software*, 66 ST. JOHN'S L. REV. 19 (1992) (arguing for greater scope of products liability theory to include software).

188. *See* R. Anderson, *Why Information Security Is Hard: An Economic Perspective*, PROC. 17TH ANNUAL COMPUTER SECURITY APPLICATIONS CONF. 358 (2001) (arguing that addressing problem of software vulnerabilities requires addressing perverse incentives in market); Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Product Liability and Other Issues*, 5 U. PITT. J. TECH. L. & POL. 1 (2004) (arguing for an establishment of a criminal legal regime to address software vulnerabilities and their fallout); Derek Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011 (2014) (suggesting an approach that would address information asymmetries in technology markets); Danielle Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CALIF. L. REV. 241 (2007) (arguing a reinvention of tort liability for software vulnerabilities should be based on changes that arose out of Industrial Age experiences); *cf.* Richard Warner & Robert H. Sloan, *Vulnerable Software: Product-Risk Norms and the Problem of Unauthorized Access*, 2012 U. ILL. J.L. TECH. & POL'Y 45 (2011) (arguing that existing legal regimes will not suffice to address software vulnerabilities, and recommends a norms-based approach).

189. *See* Concurring Statement of Acting Chairman Maureen K. Ohlhausen, *In re* Vizio, Inc., 2017 WL 527915 (F.T.C. Feb. 6, 2017) (discussing the need to analyze "more rigorously what constitutes 'substantial injury' in the context of information about consumers.").

E. Incorporate Ethics into Technology Policy

As examined above in Part II.C, through the lens of moral hazard, the opacity and ubiquity of connected devices creates a strong temptation for technology manufacturers to deceive, evade, or otherwise cheat existing policy frameworks designed to protect consumers.[190] Further, the information asymmetries between manufacturer and consumer allow manufacturers to stretch the boundaries of technological social contracts beyond their original intent.[191] Too often, the Silicon Valley philosophy of disruption has been interpreted by technology manufacturers as a license to cut ethical corners in their work and products, pushing the costs associated with the risks of this approach onto their users.

As discussed above, the innovation-over-maintenance philosophy brings with it a high degree of risk that, thus far, has generally not been borne by technology designers and manufacturers, but is rather passed on to their users and customers by default.[192] Continuing to increase the pace of technology disruption has led to actual social, economic, and legal disruption, and there is no reason to expect this pattern to change without some measure of change either from without or within, especially as the potential risks of automation, surveillance, and machine learning technologies become increasingly apparent. While beefed-up regulatory regimes are likely necessary to address these risks, at least some internal regulation must be shouldered by industry, possibly in the form of enforced ethical standards that consider societal needs and public goods.

All of the above components for resolving the cybersecurity moral hazard problem will be at best only partially effective unless a sense of justice and ethics provides the foundation to this approach. This means that lawmakers and regulators must consider both the moral and political factors that are affected by connected technologies, paying special attention to the potential social harms and threats to individual freedoms and autonomy. It also means considering human values in the same vein as we have historically considered fiscal and business value.

The idea of applying an ethical framework to software development is nothing new, of course.[193] But these proposals and frameworks limit themselves to an examination of the actions of the individual engineer, who may not always be in a position to make an ethical decision about her work, especially if that decision appears to conflict with instructions from her management. This problem is not unique to software development, and the debate about whether businesses have

190. *See, e.g.*, Mike Isaac, *How Uber Deceives the Authorities Worldwide*, N.Y. TIMES (Mar. 3, 2017), https://perma.cc/ZQQ8-G9SL; Guilbert Gates et al., *How Volkswagen's 'Defeat Devices' Worked*, N.Y. TIMES (Oct. 8, 2015), https://perma.cc/89R7-2GRV.

191. *See, e.g.*, Maggie Astor, *Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared*, N.Y. TIMES (Jul. 25, 2017), https://perma.cc/E675-EJVD.

192. *See supra* Part III.A.

193. *See, e.g.*, Don Gotterbarn et al., *Software Engineering Code of Ethics*, 40 COMM. ACM 110 (1997).

an ethical responsibility as firms, or whether that responsibility is limited to the individuals within those firms, has existed since the concept of the corporation first arose.[194] The artifacts of this ongoing debate can be found throughout the long history of corporation and business laws and policies, but of particular importance to this Article are the day-to-day pressure points applied by employers that can (and do) influence an individual's ethical choices at work.

For example, even if an individual developer has the necessary education and skills to apply secure coding practices, the decision whether or not to actually take the time to apply those practices may not entirely be her decision, and may be dependent upon the priorities and resources her management have allocated to her project. This is not a problem unique to the software industry, but a general effect of corporate hierarchical decision-making, which can—perhaps inadvertently—cause employees to take ethical shortcuts in their work.[195]

This general problem is exacerbated by the "Silicon Valley-style" of technology company management, an approach that developed with the cultures of the many technology companies that came out of that region starting in the 1970s and 1980s, and places emphasis on rapid growth and first-to-market over other priorities, too often including ethical product design and development.[196] In response to growing external public pressure to change this culture, some technology companies have begun to implement ethical compliance infrastructures, including executive-level management and company policies. To many observers of technology company culture, however, these efforts have had little—if any—effect thus far.[197]

One method that does appear to be making a difference in technology company ethical culture is a grassroots effort by the employees themselves. Individual employees at large (and powerful) companies like Amazon, Google, and Microsoft

194. In fact, this philosophical debate has origins that can be traced back to some of the core questions that arose out of the Enlightenment. *See* C. Soares, *Corporate Versus Individual Moral Responsibility*, 46 J. BUS. ETHICS 143 (2003).

195. In a 2018 study by the UK-based Institute of Business Ethics, 764 employees in the UK were asked about their organization's standards of ethical behavior, and what pressures, if any, they felt in their own ethical decision making. ETHICS & COMPLIANCE INITIATIVE, 2018 GLOBAL BUSINESS ETHICS SURVEY (2018). The two biggest factors affecting employees' ability to make their own ethical decisions were project resourcing and time availability, two areas where a company's overall budgeting decisions may have unexpected effects on employee ethical behavior. The remaining categories, however, were not as potentially benign, and included direct orders to make unethical decisions, being asked to take ethical short cuts, and a culture where they are pressured by other employees to be "team players."

196. *See supra* Part III.A.

197. *See, e.g.*, Kara Swisher, Opinion, *Who Will Teach Silicon Valley to Be Ethical?*, N.Y. TIMES (Oct. 21, 2018), https://perma.cc/7SF2-MAUY (discussing the corrupting influences of funding sources in technology companies); Evan Selinger, *Will Tech Companies Ever Take Ethics Seriously?*, MEDIUM (Apr. 9, 2018), https://perma.cc/EG4H-8PBH; Irina Raicu, *Rethinking Ethics Training in Silicon Valley*, THE ATLANTIC (May 26, 2017), https://perma.cc/W5FF-FT8X; Peter Guagenti, *Silicon Valley Has an Ethics Problem, and It Just Might Be Fatal*, INC. (Apr. 28, 2017), https://perma.cc/UGJ9-YVJG.

are applying internal pressure on their employers to put ethical decision making on the same or higher level as other priorities like profit margins.[198] This pressure has even manifested in technology companies' hiring, where prospective recruits are taking a hard look at a company's ethical track record before considering sending along an application.[199] Internal grassroots efforts such as these, where employees (and prospective employees) who are well-informed of the basics of software development ethics convince technology companies to reconsider the move-fast-and-break-things approach, may be the most immediately effective method of moving technology toward a more security-focused product cycle.

V. CONCLUSION

The proliferation of connected devices has thrown a spotlight on the problem of moral hazard that exists with cybersecurity. The deep (and growing) information asymmetries that are unique to software and related technologies have only made this problem worse. Further, in addition to the fact that the existing methods of dealing with moral hazard in other industries have proven insufficient to address cybersecurity's unique problem, the Silicon Valley philosophy of treating these sorts of large ethical issues as mere bug fixes makes a new, integrated approach to this problem necessary.

198. *See, e.g.*, Alexia Fernández Campbell, *How Tech Employees Are Pushing Silicon Valley To Put Ethics Before Profit*, VOX (Oct. 18, 2018), https://perma.cc/9LT8-WBAB; Matt Lavietes, *Silicon Valley Firms Are Facing a Rise in Anger From a New Source: Their Own Employees*, CNBC (Jul. 8, 2018), https://perma.cc/2KGK-CRY9; Joseph Menn, *Silicon Valley Employees Increasingly Push Companies on Ethics*, CHRISTIAN SCI. MONITOR (Jul. 13, 2018), https://perma.cc/NS73-L2DZ; Caroline O'Donovan, *Clashes Over Ethics at Major Tech Companies Are Causing Problems for Recruiters*, BUZZFEED NEWS (Aug. 27, 2018), https://perma.cc/5P5D-KEU8.

199. *See* Guagenti, *supra* note 197.