DEVELOPING SOFTWARE SAFETY STANDARDS

Bryan H. Choi[†]

I. INTRODUCTION

Among those who believe better software standards are needed, there is a growing schism as to who should be entrusted with developing such standards. For decades, the prevailing focus has been on whether courts ought to enforce tougher liability standards in order to promote greater discipline in software development practices.[1] A battery of doctrinal immunities, derived both from legislation and from common law, has served to shield nearly all software developers from serious scrutiny of their coding practices. Although the wisdom of such immunities has been periodically called into question, courts and legislatures alike have hesitated to unwind those brightline rules.

More recently, a new wave has arisen in favor of regulation by federal agencies as a more potent avenue for software industry reform.[2] Frustration at judicial inertia and inexpertise has caused many commentators to pin their hopes instead on agency action. The move to expand agency oversight builds upon prior agency efforts to review software quality in safety-critical domains such as avionics and medical devices.[3] Embracing this shift, the White House under

---

† Associate Professor of Law and Computer Science & Engineering, The Ohio State University. I thank Cinnamon Carlarne, Guy Rub, Chris Walker, Christopher Yoo, and Patti Zettler for helpful input at early stages of this project. I also thank Joseph van t'Hooft and Damini Mohan for excellent research assistance. This work was supported in part by NSF CCF-2131531, NSF CNS-1505799, and the Intel-NSF Partnership for Cyber-Physical Systems Security and Privacy.

[1] *See, e.g.*, Susan Nycum, *Liability for Malfunction of a Computer Program*, 7 RUTGERS J. COMPUTERS TECH. & L. 1, 8–13 (1979); Michael Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425 (2008); Frances E. Zollers et al., *No More Soft Landings for Software: Liability for Defects in an Industry that Has Come of Age*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 745, 781 (2005) (arguing that courts should apply strict liability to defective software because courts "are in the best position . . . to continue to refine and develop the doctrine as changes in technology occur").

[2] *See* RYAN CALO, BROOKINGS, THE CASE FOR A FEDERAL ROBOTICS COMMISSION 3, 11 (2014) (arguing that a centralized agency is needed to avoid a piecemeal approach); Jane Chong, *The Challenge of Software Liability*, LAWFARE (Apr. 6, 2020), https://www.lawfareblog.com/challenge-software-liability (arguing that the regulation of software security should be delegated to an agency like the Federal Trade Commission); Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2271 (2015); Paul Ohm & Blake Reid, *Regulating Software When Everything Has Software*, 84 GEO. WASH. L. REV. 1672, 1695 (2016) (worrying that software developers (or coders) will become subject to regulatory turf wars across different agencies that result in a "regulatory thicket" of inconsistent or contradictory rules); Andrew Tutt, *An FDA for Algorithms*, 69 ADMIN. L. REV. 83 (2017).

[3] *See* FAA, ADVISORY CIRCULAR 20-115 (1982) (authorizing the use of RTCA Document DO-178 as a means to secure FAA approval of digital computer software in flight control systems); FDA, GUIDANCE FOR THE CONTENT OF PREMARKET SUBMISSIONS FOR SOFTWARE CONTAINED IN MEDICAL DEVICES (2005); FDA, PROPOSED REGULATORY FRAMEWORK FOR AI-BASED SOFTWARE AS A MEDICAL DEVICE (2019); *see also* E. Stewart Crumpler & Harvey Rudolph, *FDA Software Policy*

both political parties has issued strikingly similar orders tasking the federal agencies with developing technical standards to improve the safety and trustworthiness of software systems.[4]

Yet, there is cause for caution. Despite decades of intensive study, agency regulation of software has remained so light-touch as to leave little mark at all.[5] To be sure, it is possible that the inability to articulate robust software standards is a failure only of individual agencies. Yet, if the dysfunction is shared across all agencies, then one might ask whether the agency model itself has important limitations.

This Essay considers the question of institutional choice within the context of software regulation. What lessons can the principles of institutional competence teach us about the seemingly intractable problem of software safety? Conversely, can a study of software complexity teach us anything new about institutional choice theory? Part II revisits the classic formulation of the tradeoffs between courts, agencies, and other legal institutions, as articulated by the Legal Process movement and its intellectual heirs. Part III explains the special complexity involved in software development work, which offers the best descriptive account for the present gridlock in advancing software standards. Part IV argues that, for regulatory problems like software safety where the risks and best practices are scientifically unknowable, the institutional choice question should prioritize an information-generation function.

II. INSTITUTIONAL CHOICE THEORY

In its modern incarnation, institutional choice theory posits that the choice of institution matters in shaping how policy goals turn out. The normative claim is that there ought to be a coherent theory that governs how such comparative choices should be made.[6]

The insight that different institutions have different competencies harks back to the Legal Process movement.[7] The primary impetus of that movement was to shift discretionary power away from courts to other institutions having better decision-making heuristics.[8] Accordingly,

---

and Regulation of Medical Device Software, 52 FOOD & DRUG L.J. 511, 513 (1997) (describing efforts dating back to the 1980s).

[4] *See* White House, National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, July 28, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/ (ordering the Department of Homeland Security, the National Institute of Standards and Technology (NIST), and other agencies "to develop and issue cybersecurity performance goals for critical infrastructure to further a common understanding of . . . baseline security practices"); American AI Initiative, Executive Order 13859, Feb. 2019 (ordering NIST to coordinate with other agencies in "the development of technical standards and related tools in support of reliable, robust, and trustworthy systems that use AI technologies").

[5] *See* Nathan Cortez, *Regulating Disruptive Innovation*, 29 BERKELEY TECH. L.J. 175, 192 (2014) (describing the FDA's approach to medical device software as "the archetype of regulatory minimalism"); *see also* DEF. SCI. BD., U.S. DEP'T OF DEF., REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON MILITARY SOFTWARE 24, 32 (1987) (recommending that the Department of Defense ("DoD") should retire its military software standards, because DoD "cannot expect to lead in most aspects of software technology development" and it cannot "create a *de facto* standard and impose it on the civilian market").

[6] *See* NEIL K. KOMESAR, IMPERFECT ALTERNATIVES 7 (1994) (advocating a "participation-centered approach" to comparative institutional choice); William N. Eskridge, Jr., *Expanding* Chevron*'s Domain: A Comparative Institutional Analysis of the Relative Competence of Courts and Agencies to Interpret Statutes*, 2013 WIS. L. REV. 411, 416 ("Comparative institutional analysis is normative: which institution, or cluster of institutions, will make the best rules, given the criteria for successful rules in our society or legal system?").

[7] *See* Edward L. Rubin, *The New Legal Process*, 109 HARV. L. REV. 1393, 1396 (1995) (explaining that the "central principle [of the legal process school] was that each governmental institution possesses a distinctive area of competence such that specific tasks can be assigned to that institution without reference to the substantive policies involved"); David Kennedy, *Henry M. Hart, Jr., and Albert M. Sacks*, *in* THE CANON OF AMERICAN LEGAL THOUGHT 247 (2006) ("Regulatory agencies, [Hart and Sacks] suggest, are particularly well suited for tasks requiring expertise, legislatures for those that require an ability to harness diverse social interests to a general social purpose. Appellate courts are particularly suited for monitoring these questions of institutional competence.").

[8] *See* Richard H. Fallon, Jr., *Reflections on the Hart and Wechsler Paradigm*, 47 VAND. L. REV. 953, 958 (1994) (observing that Hart and Wechsler thought the courts ill-suited "to decide 'polycentric' disputes" and "to develop policy"); William N. Eskridge, Jr. & Philip P. Frickey, *The Making of* The Legal Process, 107 HARV. L. REV. 2031, 2038 (1994) (explaining Henry

much of the commentary on judicial competency sounds in critique. Because unelected judges lack direct accountability to electoral majorities, the power of courts to dictate public policy is viewed as especially troubling.[9] As a result, the dominant stance of institutional choice theory—though by no means a universal one—has been to urge courts to defer as much as possible to the judgment and discretion of other institutions.

Challenging the competency of courts opened space for subsequent scholars to explore the relative competencies of other institutions, including agencies. Three of the most commonly discussed attributes are expertise, efficiency, and uniformity.

First, agencies are most often lauded for their ability to cultivate subject matter expertise in their respective domains, both because of their specialized missions and because of their ability to hire specialized staff with relevant training in the field.[10] Agencies are considered especially good at engaging in comprehensive fact-gathering when evaluating complex issues of public policy. By contrast, judges and juries are painted as generalists lacking in expert knowledge.[11] Moreover, judicial factfinding is limited by the cases that are filed and the evidentiary records developed through the adversarial process.[12]

Second, federal agencies are perceived to be better equipped to issue uniform rules with national reach.[13] Because agencies are organized in a top-down hierarchy, they are better at assessing systemic effects and avoiding inconsistent interpretations.[14] Courts address issues in a trickle-up fashion and are thus more likely to diverge across jurisdictions, even where there is a single governing statute.[15] While courts are capable of converging to a uniform rule, such coordination is a relative rarity.

Hart's views on the comparative advantages that legislatures and agencies have vis-à-vis courts).

[9] *See* Rubin, *supra* note 7, at 1397–98 ("Most courts, and particularly the federal courts, are more problematic because they are not directly subject to the electoral process or to the supervision of any elected official, but only to words written in a statute, a group of previous decisions, or a constitution.").

[10] *See* Eskridge, *supra* note 6, at 421–22 (explaining that agency expertise comes from specialization and from including staff who have special training); Clark Byse, *Judicial Review of Administrative Interpretation of Statutes: An Analysis of* Chevron*'s Step Two*, 2 ADMIN. L.J. 255, 258 (1988) ("Not only does the agency have a staff of technical and professional experts to assist it, but it also deals on a day-to-day basis with the regulated industry . . . ."); *see also* Sidney A. Shapiro, *The Failure to Understand Expertise in Administrative Law: The Problem and the Consequences*, 50 WAKE FOREST L. REV. 1097 (2015) (expanding the concept of agency expertise to include the "craft" expertise of "agency professionals"). *But see* Clayton P. Gillette & James E. Krier, *Risk, Courts, and Agencies*, 138 U. PA. L. REV. 1027, 1031, 1090 (1990) (pointing out that agency expertise suffers problems such as selection bias and bounded rationality, which "raises too many doubts about the wisdom of wholesale abdication to technocratic rule").

[11] *See* Peter Huber, *Safety and the Second Best: The Hazards of Public Risk Management in the Courts*, 85 COLUM. L. REV. 277, 333–35 (1985); Peter Swire, *Finding the Best of the Imperfect Alternatives for Privacy, Health IT, and Cybersecurity*, 2013 WIS. L. REV. 649, 667 (noting that courts are not a prominent alternative for many issues of privacy, security, or health information technology because these problems "concern the design of technologically complex systems," whereas courts are more expert at resolving problems about "individual redress for specific harms"). *But see* KOMESAR, *supra* note 6, at 138–40 (postulating that agencies might have superior technical expertise, but that generalist judges and juries are "less subject to systemic influence and bias").

[12] *See* Eskridge, *supra* note 6, at 413 (summarizing the critique that "judicial decision making is limited by the structure of adjudication, the kinds of parties who will litigate, and the constrained resources and limited personnel of the court system").

[13] *See* Winters, *Restoring the Primary Jurisdiction Doctrine*, 78 OHIO ST. L.J. 541, 550 (2017) (explaining the prominence of the uniformity rationale within the "primary jurisdiction" doctrine, which determines when courts should refer an issue to an administrative body for primary resolution).

[14] *See* Richard B. Stewart, *Regulatory Compliance Preclusion of Tort Liability: Limiting the Dual-Track System*, 88 GEO. L.J. 2167, 2174 (2000) ("Regulatory agencies are far better suited than lay judges and juries deciding individual cases in isolation to assess systemic risk-risk tradeoffs and strike an appropriate balance through decisions that take into account overall consequences for society as a whole.").

[15] *See* Peter Strauss, *One Hundred Fifty Cases Per Year: Some Implications of the Supreme Court's Limited Resources for Judicial Review of Agency Action*, 87 COLUM. L. REV. 1093, 1121 (1987) (stating that national agencies "can be expected to reach single readings of the statutes for which they are responsible" whereas judicial interpretations are "virtually assure[d]" to be diverse due to the Supreme Court's limited docket); Stewart, *supra* note 14, at 2169 (summarizing ALI study finding that "the tort system cannot ensure desirable consistency and coordination in legal requirements, which is especially important for nationally marketed products").

Third, agencies are usually characterized as being more efficient than courts. Because agencies operate in a command-and-control mode, they can pursue a top-down policy agenda on a speedier timeframe.[16] In principle, that unilateral model also allows agencies to be more flexible in incorporating new information based on changing developments.[17] Meanwhile, the decentralized model of common law courts requires policy changes to percolate across multiple venues, which makes any such change unpredictable.[18] Courts favor past precedent, which can lead to path dependency and delay.[19] Adjudicative action also depends on access to courts, which can be infeasible for certain constituencies.[20] The judicial process itself stands accused of being costly and wasteful.[21] To be sure, many scholars have pointed out that agencies also operate inefficiently at times, whether in relation to private market forces or to public interest ideals.[22] Nevertheless, the prevailing wisdom has been that agencies are nimbler than courts at carrying out policy agendas.[23]

In addition to studying static competencies, many commentators have cast their attention on the dynamic interactions between courts and agencies. Of those discussions, the vast majority has focused on the role of judicial review in imposing accountability on agency administrators.[24] Here, there is profound disagreement as to whether judicial review enhances agency accountability or subverts it.[25] Either way, the field of play for these arguments assumes an adversarial stance between the two institutions.[26]

The alternative stance is one of cooperative dialogue. For example, Catherine Sharkey has argued that courts should harness the expertise of agencies by embracing an "agency reference model" when determining optimal regulatory policies.[27] More expansively, Chris Walker has

---

[16] *See* Eskridge, *supra* note 6, at 419 (noting that "agencies have a variety of mechanisms that allow them to generate national rules relatively quickly: administrative rulemaking, published guidances, handbooks, and even online websites"); Tim Wu, *Agency Threats*, 60 DUKE L.J. 1841, 1848, 1851 (2011) (recommending the use of informal threats by agencies confronting conditions of "high uncertainty," and observing that "[t]he greatest advantage of a threat regime is its speed and flexibility").

[17] *See* Byse, *supra* note 10, at 259 (noting that agencies are able to change their interpretations "in light of new scientific, industrial, or other developments").

[18] See Oona A. Hathaway, *Path Dependence in the Law: The Course and Pattern of Legal Change in a Common Law System*, 86 IOWA L. REV. 601, 650 (2001) ("Legal change is unpredictable ex ante and nonergotic, and early outcomes may become locked in. . . . Opportunities for obtaining significant legal change are limited.").

[19] *See* Huber, *supra* note 11, at 307–11 (criticizing the "go slow" judicial philosophy).

[20] *See* KOMESAR, *supra* note 6, at 125 ("Judges must await action brought by moving parties, often private parties. . . . [T]he threshold costs of litigation, interacting with the distribution of stakes, can keep the courts from a given social issue or from large sets of social issues.").

[21] *See* Marc Galanter, *Real World Torts: An Antidote to Anecdote*, 55 MD. L. REV. 1093, 1140 (1996) (identifying and responding to critics of the civil justice system who are "convinced that its cost is excessive").

[22] *See* STEPHEN BREYER, BREAKING THE VICIOUS CIRCLE 10 (1993) (identifying three persistent biases of agency regulators: tunnel vision, random agenda selection, and inconsistency); Richard A. Posner, *The Rise and Fall of Administrative Law*, 72 CHI.-KENT L. REV. 953, 955–56 (1997) (identifying Naderite critiques on the left and economic critiques on the right); Wendy Wagner, *The Participation-Centered Model Meets Administrative Process*, 2013 WIS. L. REV. 671, 681 (identifying several inefficiencies in administrative process, including the cost of organizing, the cost of information, and the cost of access).

[23] *See* BREYER, *supra* note 22, at 57 ("In general courts are no more able—indeed they are less able than Congress—to consider agency agendas as a whole and to set priorities.").

[24] *See* Eskridge, *supra* note 6, at 428, 441 (stating that the "judiciary might be the best institution of all to monitor certain kinds of agency dysfunctions, including those reflecting an agency's 'minoritarian bias' in favor of its specialized perspective or that of its client groups, as well as poor decisions flowing from an agency's 'majoritarian biases' that impose unfair costs upon minorities."); Jerry A. Mashaw, *Structuring a "Dense Complexity": Accountability and the Project of Administrative Law*, 5 ISSUES IN LEGAL SCHOLARSHIP, art. 4, at 5 (2005) ("Public law—that is, administrative and constitutional law—mostly regulates regulators.").

[25] *See, e.g.*, ELIZABETH FISHER & SIDNEY A. SHAPIRO, ADMINISTRATIVE COMPETENCE 70–74 (2020) (collecting commentary).

[26] *See* Richard Nagareda, *FDA Preemption: When Tort Law Meets the Administrative State*, 1 J. TORT L. art. 4, at 3, 37 (2006) (observing that "[t]he rivalry between tort law and the administrative state arises from an increasing sense that the two regimes seek to do broadly similar things in broadly similar ways").

[27] *See* Catherine M. Sharkey, *Products Liability Preemption: An Institutional Approach*, 76 GEO. WASH. L. REV. 449, 452–53, 477–79 (2008) (advancing an "agency reference model" for judicial decisionmaking on federal preemption questions, in which "courts should look to agencies to supply the empirical data necessary to determine whether a uniform federal regulatory policy should exist").

cataloged a diverse set of tools that courts could employ to enhance court-agency dialogue.[28] In a complementary vein, Doug Kysar has offered something akin to a "court reference model," in which he defends the role of courts as a key venue where complaining parties are able to formulate unmet grievances and regulatory goals, which in turn can influence how agencies set their agendas.[29] Other scholars including Wendy Wagner, Robert Rabin, and Richard Nagareda have centered the joint role that courts and agencies can perform in generating information about risky products and activities.[30]

III. SHORTFALLS OF SOFTWARE SAFETY STANDARDS

Proposals to delegate the development of software standards to the administrative state invariably invoke these factors of expertise, uniformity, and efficiency. For example, Paul Ohm and Blake Reid have suggested that the federal government should "vest authority for code regulation in a single government agency" in order "to stamp out, or at least recognize, inconsistencies," as well as to "bring[] together experts from industry, government, the academy, and public interest groups."[31] Ryan Calo has argued that establishing a new Federal Robotics Commission would avoid the pitfalls of addressing robotics policy questions in a "piecemeal" fashion.[32] This overarching agency would "serve as a repository for expertise about a transformative technology of our time."[33] Similarly, Andrew Tutt has proposed the creation of a new "FDA for algorithms" on the grounds that a unified, federal approach would aggregate expertise and avoid a "checkerboard" of state-by-state regulation.[34] Jane Chong has argued that software security should be delegated to a new agency akin to the Federal Trade Commission (FTC), because "the complexities and uncertainties of the current, highly uneven software risk landscape" demand "consistency and coherence of efforts" to implement "industry standards and objective benchmarks."[35] Daniel Solove and Woody Hartzog agree

---

[28] *See* Christopher J. Walker, *The Ordinary Remand Rule and the Judicial Toolbox for Agency Dialogue*, 82 GEO. WASH. L. REV. 1553, 1614 (2014).

[29] *See* Douglas A. Kysar, *The Public Life of Private Law: Tort Law as a Risk Regulation Mechanism*, 9 EUR. J. RISK REG. 48, 54 (2018) (arguing that "common law tort actions can offer a decentralized and citizen-empowering means of formulating and addressing regulatory goals."); *id.* at 50 (stating that the benefits of tort adjudication are "problem articulation, norm amplification, and intergovernmental signalling"); *see also* Matthew C. Stephenson, *Public Regulation of Private Enforcement: The Case for Expanding the Role of Administrative Agencies*, 91 VA. L. REV. 93, 112 (2005) (positing that an advantage of private enforcement suits is that "[l]egal innovations pioneered by private plaintiffs, who may be more willing than conservative government agencies to experiment with new approaches, may subsequently be adopted by the government regulators themselves").

[30] *See* Wendy Wagner, *When All Else Fails: Regulating Risky Products Through Tort Litigation*, 95 GEO. L.J. 693, 695 (2007) (arguing that "the tort system plays an indispensable role in supplementing agency regulation of risky products and activities" by being "more effective than the regulatory system in accessing the various types of information needed to inform regulatory decisions"); Robert L. Rabin, *Reassessing Regulatory Compliance*, 88 GEO. L.J. 2049, 2061, 2068–70 (2000) (presenting the "information-generation mechanism" as a complementary characteristic of both the tort system and the agency regulatory system); Nagareda, *supra* note 26, at 40 (arguing that federal preemption doctrine should "work in mutual support" of information eliciting and information updating purposes); *see also* Rebecca Eisenberg, *The Role of the FDA in Innovation Policy*, 13 MICH. TELECOMM. & TECH. L. REV. 345, 370 (2007) (arguing that FDA regulation should be understood as a means of promoting investment in generating valuable information about the safety and efficacy of drugs).

[31] *See* Ohm & Reid, *supra* note 2, at 1700.

[32] Calo, *supra* note 2, at 3.

[33] *Id.* at 6; *see also id.* at 11 (proposing that the Federal Robotics Commission should "consist of a handful of engineers and others with backgrounds in mechanical and electrical engineering, computer science, and human-computer interaction" as well as experts in law and policy).

[34] *See* Tutt, *supra* note 2, at 113–14 (noting that "the most likely outcome of state-level regulation will be a checkerboard of regulatory efforts"); *id.* at 117 ("A single national agency would be able to maximize the centralized expertise that can be brought to bear on the issue while offering the most agility and flexibility in responding to technological change and developing granular solutions.").

[35] *See* Chong, *supra* note 2.

that the FTC's authority to regulate software is "sorely needed" because it is the most practical way to "establish[] some baseline standards and clos[e] gaps" in order to turn the U.S. data protection regime into "something more coherent and comprehensive.[36] Moreover, they add, the "FTC is able to consider a more complete range of concerns than those addressed by contract or tort law, and is thus able to achieve a balance that is more subtle and comprehensive of everything at stake."[37]

The top-down approach would be more compelling if the main obstacle to better software standards were merely a lack of concerted effort. But as I have explained elsewhere, the best available software standards are surprisingly lacking in substantive guidance, even in safety-critical domains such as military, avionics, and medical devices.[38] Moreover, I have argued that this failure is attributable to the exceptional complexity of software, which is unlikely to yield to top-down dictates.[39] If that root diagnosis is correct, then it implies that expertise, uniformity, and efficiency are not the key attributes to optimize when it comes to software regulation.

The U.S. military was an early frontrunner in promulgating software standards. Frustrated by problems of inconsistency and shoddy quality, the Department of Defense issued a series of mandates that its software developers should follow strict process controls in order to ensure that all military software met the requirements specified upfront.[40] These requirements would cascade like a "waterfall" from the planning stage, to the design stage, to the code implementation stage, and to the testing and integration stage. Surprisingly this top-down approach—which was adapted from best practices in other conventional engineering fields—proved unworkable in the software context. The Department of Defense was advised that it should abdicate its role in setting software standards and defer to the civilian market.[41] The military ultimately adopted this recommendation.[42]

Since the demise of the waterfall method, the dominant model of software development has been the "iterative lifecycle" approach. Instead of attempting to specify complete requirements upfront, software developers specify ad hoc requirements with the expectation that those specifications will be updated and patched in subsequent development cycles. This fragmentary approach is not considered safe or reliable, but it has proved essential to avoiding process paralysis and cost overruns. Software's commercial success has been tied intimately to this iterative model, so much so that it is baked into every modern standard on software quality.

For example, the Federal Aviation Administration (FAA) relies on the DO-178 standard to certify software used in flight control systems.[43] Early versions of this standard demanded strict waterfall design methods for the riskiest components, but those guidelines were

---

[36] *See* Hartzog & Solove, *supra* note 2, at 2271; *see also* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 642, 661–62 (2014) (endorsing expanding uses of the FTC's unfairness authority to establish baseline standards in software design and data privacy practices).

[37] Hartzog & Solove, *supra* note 2, at 2284.

[38] *See* Bryan H. Choi, *Software as a Profession*, 33 HARV. J.L. & TECH. 557, 573 (2020).

[39] *Id.* at 570.

[40] *See* U.S. DEP'T OF DEF., DOD-STD-2167, MILITARY STANDARD: DEFENSE SYSTEM SOFTWARE DEVELOPMENT 11 (1985). This standard was preceded by MIL-STD-1679, issued in 1978, and succeeded by DOD-STD-2167A, issued in 1988, and MIL-STD-498, issued in 1994.

[41] *See* DEF. SCI. BD., U.S. DEP'T OF DEF., REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON MILITARY SOFTWARE 24, 32 (1987) (recommending that the Department of Defense ("DoD") should transition to civilian standards for software, because DoD "cannot expect to lead in most aspects of software technology development").

[42] *See* Memorandum, Sec'y of Def. William Perry, Specifications & Standards – A New Way of Doing Business, June 29, 1994, *reprinted in* INSIDE THE ARMY, July 4, 1994, at 15–17 (announcing policy shift at the Department of Defense from military specifications to commercial standards).

[43] *See* FAA, ADVISORY CIRCULAR 20-115D (2017).

subsequently relaxed in order to promote greater use of software in avionics systems.[44] Since the 1992 revision, the DO-178 standard has been flexible enough that "virtually any modern methodology will suffice."[45] While the DO-178 standard provides some meaningful safeguards against low-level implementation errors, it does not provide substantive restrictions on how to plan or design software specifications.[46] In fact, to do so would clash with the iterative lifecycle model, whose basic tenet is to maximize flexibility at the planning and design stages.

Likewise, the FDA's guidance on medical device software assumes that "[m]ost software development models will be iterative."[47] Unlike the FAA, the FDA has not elected to adopt a single software standard; however, the leading international standard for medical device software development is IEC 62304, which the FDA recently endorsed as a "recognized consensus standard."[48] The IEC 62304 standard closely resembles the DO-178 standard for avionics software in key aspects. Most significantly, it too does not prescribe or proscribe any specific software development model.[49]

The iterative lifecycle model owes its uneasy durability to software's "essential complexity." [50] That complexity far exceeds conventional notions of human-designed complexity, because software is an arbitrary construct rather than one constrained by physical materials or processes. As a result, software errors do not obey a natural pattern but emerge in an arbitrary manner that cannot be rigorously tested. Moreover, the scale of software complexity typically grows much more immense than other engineering projects—and unlike the complexities encountered in physical engineering, there is no way to simplify software's essential complexity. In fact, the ease with which such complexity can be assembled is the double-edged advantage of software.

Thus, the iterative lifecycle model reflects a pragmatic understanding that software developers must be allowed to build and release software systems in incomplete increments, because software reliability cannot be assured through any standard engineering process. In most cases, even an unlimited number of iteration cycles would be insufficient to provide such assurances. Correspondingly, when software standards embrace the iterative lifecycle model, it is an implicit concession that those standards offer no meaningful assurances against software failure.

The iterative lifecycle model might be less problematic if there were easily quantifiable performance measures that could simplify the assessment of software safety. [51] As a

---

[44] *See* RADIO TECH. COMM'N FOR AERONAUTICS, DO-178C, SOFTWARE CONSIDERATIONS IN AIRBORNE SYSTEMS AND EQUIPMENT CERTIFICATION app. A (2011) (explaining that the 1992 DO-178B revision arose out of a desire to incorporate "rapid advances in software technology"); J.P. Potocki de Montalk, *Computer Software in Civil Aircraft*, 17 MICROPROCESSORS & MICROSYSTEMS 17, 21 (1993) (acknowledging that the 1985 DO-178A standards are "extremely severe, and require the structure of the software to be simple and deterministic").

[45] VANCE HILDERMAN & TONY BAGHI, AVIONICS CERTIFICATION 54 (2011).

[46] *See* RTCA, DO-178C, *supra* note 44, at 21–22 ("This document does not prescribe preferred software life cycles and interactions between them. . . . The processes of a software life cycle may be iterative, that is, entered and re-entered. The timing and degree of iteration varies due to the incremental development of system functions, complexity, requirements development, hardware availability, feedback to previous processes, and other attributes of the project."); *id.* at 26 ("Other software life cycle processes may begin before completion of the software planning process . . . .").

[47] *See* FDA, GENERAL PRINCIPLES OF SOFTWARE VALIDATION; FINAL GUIDANCE FOR INDUSTRY AND FDA STAFF 19 (2002); *see also id.* at 1 (declining to "recommend any specific life cycle model or any specific technique or method").

[48] *See* FDA, Recognized Consensus Standard No. 13-79, Jan. 14, 2019, https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfstandards/detail.cfm?standard__identification_no=38829; *see also* INT'L ELECTROTECHNICAL COMMISSION, IEC 62304: MEDICAL DEVICE SOFTWARE – SOFTWARE LIFE CYCLE PROCESSES (2006).

[49] *See* Nadica Hrgarek, *Certification and Regulatory Challenges in Medical Device Software Development*, 4 INT'L WORKSHOP ON SOFTWARE ENG'G IN HEALTH CARE 40, 42 (2012) ("CEI/IEC 62304 does not prescribe a specific software development life cycle model to be used during development and maintenance of medical device software.").

[50] *See* Choi, *supra* note 38, at 570 (citing Frederick P. Brooks, Jr., *No Silver Bullet: Essence and Accidents of Software Engineering*, COMPUTER, Apr. 1987, at 10, 10).

[51] *See* RTCA, DO-178C, *supra* note 44, at 12 ("Development of software to a software level does not imply the assignment of a failure rate for that software. Thus, software reliability rates based on software levels cannot be used by the system safety

comparison, environmental safety is a complex, polycentric problem, but it is relatively straightforward to measure usage and emissions of targeted pollutants. Pharmaceutical safety is similarly complex, yet beneficial effects and adverse effects can be tracked even when the biological mechanisms are poorly understood. Traffic safety has been reduced to simplistic measurements such as fatalities per hundred million vehicle miles traveled. For software safety, such quantifiable performance measures have eluded discovery.[52]

When commentators invoke federal agencies as an ideal forum for developing new software standards, they commonly invoke competencies such as expertise, uniformity, and efficiency. But those values offer less salience here. The pivotal problem is not one of inefficient coordination of expertise. As long as software's "essential complexity" necessitates an iterative lifecycle approach to software development, a top-down regulatory approach will fare no better than prior efforts by experts to develop software safety standards. Aggregating expertise within a single federal agency will yield only the same outcome that agencies like FAA and FDA—and private bodies like ISO, IEC, and IEEE—have already settled on. Contrary to the hope for a uniform approach, any standards that emerge would likely continue to delegate discretion to individual software developers to plan and design software systems in ad hoc, iterative fashion.

IV. THE INFORMATION-CENTERED APPROACH

For safety domains such as software where the likelihood of bad outcomes cannot be scientifically determined, I have advocated instead a bottom-up approach that requires experts to grapple with and opine on individual cases of harm.[53] By doing so, the software community receives a detailed factual record regarding real-world software systems, and the specific planning and design choices leading up to the software failures in question. Importantly, it induces software experts to reflect, in an adversarial setting, on actual norms and customary practices within the software industry.[54] Over time, that dialogue builds a body of knowledge as to which real-world practices are tolerated and which ones are consistently condemned by the community of software developers.

A helpful example comes from the multidistrict litigation against Toyota involving claims of unintended acceleration by its vehicles. A joint investigation by the National Highway Traffic Safety Administration (NHTSA) and by NASA had ruled out software-related causes, and had concluded that the unintended acceleration events were caused primarily by mechanical errors such as "pedal misapplication" or "pedal entrapment."[55] The ensuing litigation, however, produced expert testimony that raised numerous red flags about Toyota's

---

assessment process in the same way as hardware failure rates. . . . It is important to realize that the likelihood that the software contains an error cannot be quantified in the same way as for random hardware failures."); *id.* at 89 ("Many methods of predicting software reliability based on developmental metrics have been published . . . . This document does not provide guidance for those types of methods, because at the time of writing, currently available methods did not provide results in which confidence can be placed.").

[52] *See* Choi, *supra* note 38, at 583.

[53] *See id.* at 614 (arguing that courts invoke the customary care standard when, inter alia, "bad outcomes are mainly attributable to inherent uncertainties in the science of the profession"); *cf.* RTCA, DO-178C, *supra* note 44, at 89 (declaring that "equivalent safety" for the software can be demonstrated through a review of the software's "product service history" to show the "types of problems occurring during the service history period").

[54] *See* Choi, *supra* note 38, at 617–18 (positing that the customary care standard would generate information on worst practices, as well as generate information on the range of practices in areas where there is no established custom).

[55] *See* NHTSA, DEP'T OF TRANSP., TECHNICAL ASSESSMENT OF TOYOTA ELECTRONIC THROTTLE CONTROL (ETC) SYSTEMS 31 (2011) ("NHTSA believes that these incidents are very likely the result of pedal misapplication" or "a stuck accelerator pedal"); *id.* at 60 (noting that "[e]xtensive software testing and analysis was performed" and that "software defects that unilaterally cause a UA [unintended acceleration] were not found").

software development practices. The experts questioned why Toyota had failed to record software failures or diagnostic codes that might be relevant to replicating or testing the unintended acceleration issue.[56] The experts also criticized other practices such as extensive use of global variables, and the decision not to follow coding standards used by other major auto manufacturers.[57] While the experts were unable to pinpoint a specific defect, the court found their testimony sufficient that a reasonable jury could infer a defect's existence, particularly "in light of the fact that [Toyota's] software does nothing to track its own failures."[58] Setting aside the specific result of this case, the litigation produced a conscientious, independent code review with a reasoned elaboration of which aspects of Toyota's software development practices should be found problematic.[59] And although the experts in the Toyota case focused on basic, low-level deficiencies, it provides a template for how experts in other cases could elevate their review to higher-level elements.

Not all expert opinions are equally credible. In another case involving a baby monitor device accused of failing to sound an alarm due to a software defect, plaintiffs hired three experts to evaluate the device's software source code.[60] The experts testified that the software consisted of "spaghetti code"—in other words, that the code was so disorganized as to be indecipherable. Yet, one expert "admitted that he never examined the code in any detail and only 'spent a half an hour thumbing through it and looking at it.'"[61] A second expert stated that "it was not his job to look through the code for errors."[62] The third expert purported to conduct a code review, but his conclusory statements showed that he had simply assumed his conclusion.[63] A more searching review of the actual code and supporting documentation might have helped identify which software development practices should be considered problematic, and why.

This tilt toward courts rather than agencies can be defended in the software safety context by adopting an information-centered approach to institutional choice. The information-centered approach is distinguishable from other theories such as the participation-centered approach,[64] because it prioritizes the generation of new evidentiary information, rather than seeking to maximize the participation of interested parties. Ordinarily the two approaches share a natural overlap: greater participation by interested parties can help amass the best available information about a given regulatory problem.[65] But the information-centered approach differs where scientific knowledge is at its muddiest. In such scenarios, an agency's ability to marshal subject matter expertise provides no advantage in forging a regulatory path forward. Instead, the judicial process can be more proficient than the administrative process at generating an alternate type of information: evidentiary records from adversarial proceedings.

Doug Kysar offers the example of fruit growers seeking to eliminate harmful emissions from a nearby aluminum facility during the 1960s, prior to enactment of the Clean Air Act.[66]

---

[56] In re Toyota Motor Corp. Unintended Acceleration Litig., 978 F. Supp. 2d 1053, 1094, 1101 (C.D. Cal. 2013).
[57] *Id.*
[58] *Id.* at 1102.
[59] *Cf.* Kysar, *supra* note 29, at 50 ("Even when a plaintiff's case fails on the merits, judicial engagement with the details of her claim helps to frame her suffering as a legible subject of public attention and governance."); Wagner, *supra* note 31, at 714 (arguing that even the "worst cases" of regulatory litigation have information-production virtues that outweigh their costs).
[60] Graves v. CAS Med. Sys., 735 S.E.2d 650 (S.C. 2012).
[61] *Id.* at 72.
[62] *Id.* at 72.
[63] *Id.* at 71, 76 (finding that this expert "simply assumed the alarm did not sound and provided no reason for discounting the evidence to the contrary other than the assertion of the person alleging a failure").
[64] *See* KOMESAR, *supra* note 6.
[65] *See* Wagner, *supra* note 22, at 674–75 (explaining that "robust participation ensures that all groups have access and a voice, which gives the forum legitimacy," while also providing institutional decisionmakers with "a more complete base of information from which to make decisions").
[66] *See* Kysar, *supra* note 29, at 58.

Though the defendant argued that the cost of preventing emissions would be prohibitively expensive, plaintiffs developed an extensive evidentiary record showing that an alternative approach to pollution control was feasible and effective.[67] The generalized problem of air pollution may have been daunting and scientifically uncertain, but facing off against a specific factory with a defined approach impelled the plaintiffs to articulate unexplored deficiencies with that approach.

Similarly, the common understanding among software experts is that the cost of preventing software failures is prohibitively expensive. As a consequence, within the ad hoc framework of the iterative lifecycle model, a remarkably vast array of software development practices has sprung into existence and has been presumed to be equally acceptable. The adversarial process could reveal where the true bounds of acceptability lie. Here, the heterogeneity of the judicial process serves as an institutional advantage, not a disadvantage. Where the science of the field offers no firm guidance, the search for safety standards should tolerate a range of practices. The surest way to locate that range is on a case-by-case basis.

Agencies continue to play an important role under the information-centered approach. As many commentators have observed, agencies and courts work dynamically together to generate evidentiary information across many regulatory contexts.[68] In the environmental context, the approach pioneered by the fruit growers' litigation has become tightly embedded into the administrative work of the EPA. Likewise, agencies such as FAA, FDA, and NHTSA should incorporate the lessons of software safety litigation. These agencies also perform their own investigative and adjudicative functions, which can provide a parallel track for generating evidentiary information. But those agency activities should be viewed as complementary to, not substitutive of, the information-generating role of courts.[69]

Relying on courts to generate evidentiary information is not without its own substantial risks. One important risk is that defendants will repeatedly choose to settle rather than to litigate close cases. Settlement avoids or suppresses the discovery process that is crucial to providing independent reviews of software development practices.[70] Second, even if a case undergoes the discovery phase, defendants might misuse evidentiary rules to elude adversarial review.[71] A third risk is that courts will resolve software safety claims on summary grounds, whether in favor of plaintiffs or defendants, thus obviating the need for searching discovery.[72] Thus, courts attentive to the information-centered approach should pay close scrutiny to questions of how information about software systems and software development practices is obtained, reviewed, and released.

---

[67] *Id.* at 62–63 (citing Renken v. Harvey Aluminum Inc., 226 F. Supp. 169 (D. Or. 1963)).

[68] *See* Wagner, *supra* note 30, at 696 ("Once the information needed to inform regulation is made available through tort litigation, the work of the tort system is done. Regulators must then re-enter the process and develop more sophisticated and streamlined approaches to product regulation . . . .").

[69] *Cf.* Rabin, *supra* note 30, at 2074 ("[N]o serious commentator would argue for a regulatory compliance defense in circumstances where the agency regulations are regarded as minimum safety standards rather than optimal standards.").

[70] *See* Nora Freeman Engstrom, *Sunlight and Settlement Mills*, 86 N.Y.U. L. REV. 805 (2011); Wagner, *supra* note 31, at 731 (stating that "the practice of sealing documents in the course of settlements has the potential to undermine significantly the information-generating benefits of regulatory litigation").

[71] *See* Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018); Rebecca Wexler, *Privacy as Privilege: The Stored Communication Act and Internet Evidence*, 134 HARV. L. REV. 2721 (2020).

[72] *Compare* Scott, *supra* note 1, at 450–57, 470–71 (describing summary dismissals of software tort claims based on the economic loss doctrine and contractual preclusion), *with* Jonathan M. Hoffman, *Res Ipsa Loquitur and Indeterminate Product Defects: If They Speak for Themselves, What Are They Saying?*, 36 S. TEX. L. REV. 353 (1995) (describing the allowance of circumstantial evidence to prove likelihood of product defect).

V. CONCLUSION

The impulse to propose a super-agency for software regulation stems from optimism about the special competencies of administrative agencies, as well as pessimism about other institutions, including courts and the private market. This Essay seeks to moderate that exuberance by explaining that agencies offer few if any comparative institutional advantages in the arena of software safety, while courts offer more comparative advantages than usually supposed.

The conventional advantages of agencies are expertise, uniformity, and efficiency. Yet, software experts have already labored extensively to develop uniform standards that certify software quality. Those efforts point to an overwhelming consensus that a top-down regulatory approach will not work for the software safety domain, because software is too complex to be planned and designed in a comprehensive manner. There is little reason to suspect that agency experts would reach a different conclusion.

Ordinarily, the institutional choice analysis might end there. But an information-centered approach suggests that courts may have a latent comparative advantage in domains such as software safety where the risks are scientifically indeterminable. By generating evidentiary information about specific software systems and software development practices in an adversarial setting, courts can force the software community to confront the full range of real-world practices and to opine on the bounds of acceptability. This bottom-up wellspring of information can then be used by agencies or other regulators to locate a minimum floor of unacceptable practices, even while experts cannot agree on what are good practices.

The information-centered approach strongly suggests that courts must embrace a more proactive role in overseeing software liability cases. In that regard, I align myself with those commentators who have called for deeper judicial engagement in software tort cases. But unlike those commentators, I do not necessarily believe deeper judicial engagement needs to correlate with higher liability rates. The information-generation function is outcome-neutral, and is served equally well regardless whether liability attends.