REVISITING REASONABLE CYBERSECURITY

Jeffrey L. Vagle†

Prospective theories of cybersecurity liability have traveled over some well-worn paths over the past three decades, resulting in some successes, but also in at least as many cul-de-sacs and dead ends. Part of this problem can be found in the difficulty and complexity of the subject itself. Courts, legislators, and regulators all face comprehension difficulties when they attempt to fit our existing legal system around cybersecurity, often resulting in half-measures and generalized solutions that are challenging to apply to the widely different technical details behind each case. And in the background, we have a general reluctance to create legal regimes that might unnecessarily hinder the technology industry.

The resulting legal landscape for cybersecurity is an incoherent and ineffectual mess. But as our political, military, economic, infrastructural, and social systems continue to increase their dependency on potentially insecure software and hardware, our timidity and indecision around cybersecurity liability incurs greater real-world harms. Because of our muddled and incomplete cybersecurity legal frameworks, the associated costs are not necessarily borne by the appropriate or most culpable parties. The gaps in our current legal and regulatory frameworks make it next to impossible to consistently and reliably apportion damages or apply incentives and reduce cybersecurity policies to a series of wish lists.

This Article means to advance the cybersecurity liability conversation by taking another look at what are considered "reasonable" cybersecurity practices informed by current accepted frameworks, regulatory decisions, case law, policy goals, and other lessons learned. The Article will rely heavily on common law standards of reasonableness, but will also look to standards used within other legal theories and policy frameworks. This Article borrows useful components of

† Georgia State University College of Law. The author would like to thank Steve Bellovin, Bryan Choi, Jeff Kosseff, Susan Landau, Alan Rozenshtein, Josephine Wolff; the organizers and participants of the 2023 Cybersecurity Law and Policy Scholars Conference; the faculty at the University of Oklahoma College of Law; and the participants of the 2024 Georgia State University College of Law Faculty Workshop.

reasonableness from an array of sources to derive a test to assess the reasonableness of cybersecurity-related actions and choices. This test is meant to provide a flexible standard that is technically grounded, empirically precise, yet accessible enough for courts and lawmakers to fairly apply to cybersecurity cases that are sure to present new challenges as our technologies continue to evolve.

TABLE OF CONTENTS

INTRODUCTION

The concept of reasonableness is everywhere in the American legal system. In common law, reasonableness provides the basis for multiple theories crafted to create a balance between the competing interests of tort litigants.[1] Similarly, expectations of performance required by contracts rely heavily on what reasonableness demands. Our Constitution specifically includes references to what is reasonable when considering government intrusions on citizens' private lives and appropriate punishments for criminal acts. Reasonableness standards are widely found throughout commercial law, employment law, tax law, bankruptcy law, corporate law, and our rules governing civil procedure.[2]

Traditionally, reasonableness has proven attractive as a legal standard due to its basis in objectivity.[3] Where societal values and norms are based on respect for individual rights, a test for reasonableness can provide what appears to be a neutral boundary between the freedom of

---

1 *See* Duncan Kennedy, *Form and Substance in Private Law Adjudication*, 89 HARV. L. REV. 1685, 1747 (1976) ("[The] plausibility . . . [of natural economic interactions under property and contract law] was based on the combination of the belief that the substantive content of the common law rules was an embodiment of the idea of freedom with the belief that official intervention to enforce the rules was nondiscretionary. The basis of the first belief, as we have seen, was conceptualism. The second notion expressed itself through a complex of doctrines, including stare decisis, the nondelegation doctrine, the void for vagueness doctrine, objectivism in contracts, the reasonable person standard in torts, the distinction between questions of law and questions of fact, and the general idea that law tended to develop toward formally realizable general rules.").

2 *See, e.g.*, Imad D. Abyad, *Commercial Reasonableness in Karl Llewellyn's Uniform Commercial Code Jurisprudence*, 83 VA. L. R. 429, 443–51 (1997) (describing the use of "commercial reasonableness" in Uniform Commercial Code Article 2); David Benjamin Oppenheimer, *Negligent Discrimination*, 141 U. PA. L. REV. 899, 963–64 (1993) (noting the uses of the "reasonable person" and "reasonable woman" standards in employment discrimination cases); Mark J. Roe, *Bankruptcy and Debt: A New Model for Corporate Reorganization*, 83 COLUM. L. REV. 527, 533 (1983) (discussing the reasonableness standard for levels of debt appropriate in bankruptcy reorganizations); Melissa L. Nelken, *Sanctions Under Amended Federal Rule 11—Some 'Chilling' Problems in the Struggle Between Compensation and Punishment*, 74 GEO. L.J. 1313, 1340–41 (1986) (describing the reasonable inquiry standard of Federal Rules of Civil Procedure Rule 11).

3 *See, e.g.*, Kevin P. Tobia, *How People Judge What is Reasonable*, 70 ALA. L. REV. 293, 304 (2018) (noting how reasonableness, seen through a virtue ethics lens, sees the standard as an "objective[,] normative standard").

private activities and the harms that result from the interactions between free individuals. Where someone's conduct harms another, whether intentionally or otherwise, some form of regulation of such conduct is a necessary interference with what would otherwise be protected individual behavior. The objectivity of such behavioral regulation is maintained through an interpretation of reasonableness, a standard that can be evaluated based on the facts of the case and will account for what is contextually considered usual and customary.[4] Reasonableness, then, provides us with an objective balance between our desire for individual freedoms and our desire for security from harm.

But reasonableness as a legal standard when it comes to claims relating to cybersecurity failures has proved elusive in many contexts, with significant disagreement among technical and legal experts, practitioners, and policymakers as to the exact dimensions of such a standard, due in large part to the sheer complexity—legal, social, and technical—of the problem. Part of this issue has historical roots in protectionist attitudes toward the United States technology industry. Other obstacles arise from disagreement over the nature of software itself. Still others arise out of legal doctrines that limit or prevent certain claims, contract terms that indemnify firms, and the difficulties inherent in convincing courts of harms or injuries that do not fit neatly into prior models or fail to be readily analogized to them.

Calls to strengthen accountability for cybersecurity failures have steadily increased over the decades, with marginal success.[5] Economic harms, both collective and individual, have long been apparent to courts, but injuries that are not so easily translated into a dollar value have been met with a high degree of skepticism, even with a growing consensus among the public at large whose day-to-day lives increasingly depend on complex, opaque systems of software and hardware with security that may fail for reasons people cannot understand or necessarily control.[6] And the systems that operate and control industrial, utility, and other critical infrastructures are not necessarily more secure than their consumer counterparts, a fact which has drawn state and federal governments into the conversation about what should be considered reasonable cybersecurity.[7]

---

4 *See* Joseph William Singer, *The Legal Rights Debate in Analytical Jurisprudence from Bentham to Hohfeld*, 1982 WIS. L. REV. 975, 1029–31 (1982).

5 *See infra* Section I.B.

6 *Id.*

7 *See generally* WOLFGANG SCHWAB & MATHIEW POUJOL, THE STATE OF INDUSTRIAL CYBERSECURITY (2018); A. Creery & E.J. Byres, *Industrial Cybersecurity for Power System and SCADA Networks* (Petrol. & Chem. Indus. Conf., IEEE Indus. Applications Soc'y, Working Paper No. PCIC-2005-DV45, 2005).

This Article takes a fresh look at a cybersecurity reasonableness standard, building upon the broad foundation of work that has been done, and continues to be done, in this field. Part I provides the background to this problem and the major challenges faced when considering data security cases and argues that a usable standard of cybersecurity reasonableness is necessary to begin addressing these issues. The harms that emerge from cybersecurity cases are increasingly significant, a problem that will continue to grow as computers infiltrate our physical lives and not just our digital ones.

Part II begins with a short refresher on reasonableness in the contexts that apply most directly to the challenge of cybersecurity accountability: common law and regulatory sources, paying attention to important industry standards and best practices at the same time. Further, while this Article will not dwell extensively on the important role of regulation in cybersecurity,[8] it will pay special attention to the beneficial feedback loop that exists between tort liability and government regulation and how reasonableness in one area can help guide that standard in another. More specifically, this Article will examine the use of "best available technology" standards in environmental regulation with an eye toward their application as a cybersecurity reasonableness standard, especially in the context of negligence and negligence per se claims.[9]

Finally, in Part III, this Article takes the useful components of reasonableness from this array of sources to derive a five-part test to assess the reasonableness of cybersecurity-related actions and choices. This test is meant to provide a flexible standard that is technically grounded and empirically precise, yet accessible enough for courts and lawmakers to fairly apply to cybersecurity cases that are sure to present new challenges as our technologies continue to evolve.[10]

It is important to note here that the goal of this Article is to help advance the ongoing conversation regarding accountability for cybersecurity failures, mainly through a reevaluation of reasonableness in relevant contexts. Historically, the rules we apply to questions of liability,

---

8 *See, e.g.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 666–70 (2014); Ari Ezra Waldman, *Privacy's Rights Trap*, 117 NW. U. L. REV. ONLINE 88, 91 (2022) ("I am not prepared to give the information industry the gift of weak regulation. Nor should policymakers legitimize a subordinating, data-extractive business model simply because they have no better ideas than individual rights."); Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 613–15 (2021); Fabio Ramazzini Bechara & Samara Bueno Schuch, *Cybersecurity and Global Regulatory Challenges*, 28 J. FIN. CRIME 359 (2021); Michael J. Glennon, *The Dark Future of International Cybersecurity Regulation*, 6 J. NAT'L SEC. 563 (2013).

9 *See infra* Section II.E.

10 *See infra* Part III.

especially when they concern new technologies or new uses of existing technologies, have not been handed down to us, fully formed like Athena from Zeus. They are instead created through years or decades (or more) of decisions by courts, legislators, and regulators, and often require multiple iterations before these rules meet the needs they were originally intended to address. Such is the case with cybersecurity. While we cannot help but acknowledge the many obstacles that have historically faced those seeking to bring cybersecurity liability claims, we should not be concentrating only on the specific systemic changes that are necessary to remove these obstacles. It is also helpful to build a kind of framework, based largely on common law, that better describes the reasonableness standards we should be applying when it comes to the security of the technological systems upon which our daily lives increasingly depend.

I. WHY REASONABLENESS MATTERS TO CYBERSECURITY

Reasonableness, in the context of jurisprudence, serves two principal purposes. First, legal standards based on reasonableness help us, through courts and juries, to assess liability in as objective a way as possible. We do not ask how a defendant or plaintiff themselves should subjectively act, but instead, we compare their actions to those of a reasonable person, a legal fiction necessary to provide a kind of framing needed to see things from the most fair or equitable perspective. Second, reasonableness as a standard allows us to incorporate community and social values as we now see them, which may not be the same notion of reasonableness our forebears held in past decades or centuries. The things we view positively now may have been abhorrent to previous generations. Similarly, regional and cultural differences may also be considered by this standard. Without a notion of reasonableness, our legal system would look quite different and would likely have a rigidity that would require much more cumbersome frameworks.[11] The application of the standard can change without changing the actual language of the standard.

For some time now, we have been getting deeper into that part of the innovation cycle where the gaps between our legal and regulatory structures and the novel questions about liability that arise from the introduction and use of new technologies have become quite noticeable. It gets progressively easier over time to come up with examples of

11 This is not to say that reasonableness, being an inexact metric, is not without its problems. This Article argues that it does, however, tend to outweigh negative aspects through these two key characteristics.

harms—or negative externalities—that stem from insecure software.[12] For decades, scholars, practitioners, and advocates have articulated the many ways in which cybersecurity failures are harmful within a society that is increasingly technology dependent.[13] And with new technologies, as new (and sometimes unexpected) uses of those technologies arise, new threats emerge from the loss of security in those technologies. Most recently, software, once limited to the ethereal world of memory chips and computer storage devices, has been rapidly showing up in the physical world, controlling things like cars, drones, and medical devices, where cybersecurity failures can result in actual human injury or even death.[14] These harms can have serious national security implications as well, a fact that governments continuously wrestle with.[15]

The approach in the United States to the problem of cybersecurity failures has been largely one of laissez-faire, self-regulation, or light-touch regulation.[16] But these approaches have begun to show their age,

---

12 *See, e.g.*, Ioannis Agrafiotis, Jason R. C. Nurse, Michael Goldsmith, Sadie Creese & David Upton, *A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate*, J. CYBERSECURITY, Sept. 2018; Michael Chertoff, *Cyber Risk is Growing. Here's How Companies Can Keep Up*, HARV. BUS. REV. (Apr. 13, 2023), https://hbr.org/2023/04/cyber-risk-is-growing-heres-how-companies-can-keep-up [https://perma.cc/YJ8E-25HP].

13 *See, e.g.*, Mark Verstraete & Tal Zarsky, *Cybersecurity Spillovers*, 47 BYU L. REV. 929 (2022); Derek E. Bambauer, *Schrödinger's Cybersecurity*, 48 U.C. DAVIS L. REV. 791 (2015); Michael Warner, *Cybersecurity: A Pre-History*, 27 INTEL. & NAT'L SEC. 781 (2012); Julie E. Cohen, *The Regulatory State in the Information Age*, 17 THEORETICAL INQUIRIES L. 369 (2016).

14 *See* Bryan H. Choi, *Crashworthy Code*, 94 WASH. L. REV. 39, 39, 49–50 (2019); Rasim Alguliyev, Yadigar Imamverdiyev & Lyudmila Sukhostat, *Cyber-Physical Systems and Their Security Issues*, 100 COMPUTS. INDUS. 212, 212–13 (2018); Rebecca Crootof, Margot E. Kaminski & W. Nicholson Price II, *Humans in the Loop*, 76 VAND. L. REV. 429, 458, 492 (2023).

15 *See, e.g.*, Jill McKeon, *Biden Administration Unveils National Cyber Workforce and Education Strategy*, TECHTARGET (July 31, 2023), https://www.techtarget.com/healthtechsecurity/news/366593974/Biden-Administration-Unveils-National-Cyber-Workforce-and-Education-Strategy [https://perma.cc/3U5D-YPNT] (noting the strategy's goal to "equip every American with foundational cyber skills, transform cyber education, expand and enhance the national cyber workforce, and strengthen the federal cyber workforce"); Ryan Naraine, *US Senator Wyden Accuses Microsoft of 'Cybersecurity Negligence,'* SEC. WEEK (July 27, 2023), https://www.securityweek.com/us-senator-wyden-accuses-microsoft-of-cybersecurity-negligence [https://perma.cc/4YCF-DAW5].

16 *See* Llewellyn Joseph Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 CORNELL J.L. & PUB. POL'Y 475, 484 (1997) ("Ultimately, the strongest argument for self -regulation is that it works. Under the current laissez-faire approach, cyberspace has experienced exponential growth measured by the total number of users, total volume or dollar value of commerce, and the advancement of the technology. Further, the technology, software, and infrastructure has responded virtually instantaneously to meet every perceived need or to protect against perceived dangers. Thus, experience in cyberspace militates for a hands-off approach by government."); EV EHRLICH, PROGRESSIVE POL'Y INST., A BRIEF HISTORY OF INTERNET REGULATION 4–5 (2014), https://www.progressivepolicy.org/wp-content/uploads/2014/03/2014.03-Ehrlich_A-Brief-

especially as our technologies have expanded in ways likely unanticipated, even only two or three decades ago. This has led to a number of failures to address the growing cybersecurity problem, with the Obama administration acknowledging as much in 2013, with Executive Order 13,636 and Decision Directive 25, calling for a hybrid model that gives the right incentives—carrots and sticks—to manufacturers as least-cost avoiders in the technology marketplace.[17]

It would make sense, therefore, that, given our objective models of reasonableness that make up our legal system, we would be applying these models to ensure the costs of cybersecurity harms are borne by the appropriate parties, that incentives are properly set to ensure manufacturers are applying proper security measures to their products, and we would be better able to contain some of the larger network effects that emerge from technology security failures.[18] Calls for greater cybersecurity measures can be found daily in newspapers, political speeches, and expert opinions, so it would appear as if moves to create legal accountability for cybersecurity failures would be a foregone conclusion at this point.[19]

History-of-Internet-Regulation.pdf [https://perma.cc/UC8T-BU3N] ("The Clinton Administration . . . believed strongly that relying on private investment and markets would be the best route to promoting innovation . . . . [This perspective was made manifest in] the Telecommunications Act of 1996[,] . . . [a] watershed event that marked the end of the telephone age and the beginning of the Internet age . . . .").

17 INTERNET SEC. ALL., THE CYBER SECURITY SOCIAL CONTRACT: POLICY RECOMMENDATIONS FOR THE OBAMA ADMINISTRATION AND 111TH CONGRESS (2008), https://obamawhitehouse.archives.gov/files/documents/cyber/ISA%20-%20The%20Cyber%20Security%20Social%20Contract.pdf [https://perma.cc/LQ8K-8CDP] (explaining that traditional modes of information transmission in the government do not work for cybersecurity); Nelly Rosenberg, *An Uphill Battle: FTC Regulation of Data Security as an Unfair Practice*, 66 DEPAUL L. REV. 1163, 1171–72 (identifying the patchwork agency jurisdictions that characterize poor cybersecurity policy).

18 *See* Jeffrey L. Vagle, *Cybersecurity and Moral Hazard*, 23 STAN. TECH. L. REV. 71, 108–11 (2020).

19 *See Secure By Design*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/securebydesign [https://perma.cc/K9EY-F2Y7] (gathering a collection of documents describing the problem of poor security design and development practices and how best to address them); Bob Lord & Jack Cable, *Leading the Way with Radical Transparency*, CISA BLOG (July 18, 2023), https://www.cisa.gov/news-events/news/leading-way-radical-transparency [https://perma.cc/7ZT2-ZWHL] ("We talk a lot about a future where market forces drive stronger security, but to make this a reality, we need to be able to evaluate products based on their security. And we certainly haven't made that easy for customers to date. As it stands, too often security claims are written by marketing teams and not based on actual evidence. For instance, marketing teams often claim 'military grade encryption' when in reality, military grade encryption is no different from standard encryption, but how could a hospital system, a water treatment facility, or a school district know this?"); Tim Starks & David DiMolfetta, *Cybersecurity Labels for Smart Devices Are on Their Way*, WASH. POST (July 18, 2023, 7:01 AM), https://www.washingtonpost.com/politics/

The statutory language of data security-related regulatory and legislative efforts depends on some understanding of reasonable cybersecurity. The California Consumer Protection Act (CCPA), effective January 1, 2023, gives California residents a private right of action if their personal information is revealed through a data breach that is the result of a company's failure to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information."[20] Colorado's 2018 cybersecurity law requires covered entities to maintain "reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations."[21] New York's 2019 Stop Hacks and Improve Electronic Data Security (SHIELD) Act requires companies to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity" of private information.[22] Ohio's 2018 Data Protection Act requires covered entities to "reasonably conform[] to an industry recognized cybersecurity framework."[23] These examples provide varying degrees of guidance as to what "reasonable" might mean in these contexts, but they often leave as many questions as they do answers.[24]

Two instructive examples of the application of reasonableness standards to cybersecurity-related scenarios can be found in the *Federal Trade Commission v. Wyndham Worldwide Corporation* and *LabMD,*

2023/07/18/cybersecurity-labels-smart-devices-are-their-way [https://web.archive.org/web/20240920190157/https://www.washingtonpost.com/politics/2023/07/18/cybersecurity-labels-smart-devices-are-their-way] ("The Trust Mark label will go to products that demonstrate common safeguards, like software updates and unique, strong default passwords, as spelled out by the National Institute of Standards and Technology . . . ."); Robert William Wilkins, *Four Tips to Avoid Denial of Cyber Insurance Coverage for a Data Breach*, AM. BAR ASS'N (Jan. 31, 2023), https://www.americanbar.org/groups/litigation/committees/commercial-business/practice/2023/four-tips-avoid-denial-cyber-insurance-data-breach [https://web.archive.org/web/20240419060728/https://www.americanbar.org/groups/litigation/resources/newsletters/commercial-business/four-tips-avoid-denial-cyber-insurance-coverage-data-breach] ("[S]ome of the key items insurance providers require for coverage include the use of multifactor authentication, employee training on phishing and other types of cyberattacks, strength-of-password requirements, regulatory reporting obligations, as well as an assessment of the quality of the insured's incident-response plan and penetration testing. The insured's compliance with the requirements is required to keep the coverage."); *Avoiding the Most Common Cyber Insurance Claim Denials*, GB&A INS., https://www.gbainsurance.com/avoiding-cyber-claim-denials [https://perma.cc/4M4A-WARW] ("Often referred to as the negligence or 'failure to follow' exclusion, some carriers contain within their policy language, a specific exclusion which precludes coverage for claims arising from the insured's failure to maintain minimum/adequate security standards.").

20 CAL. CIV. CODE § 1798.150(a)(1) (West 2023).

21 COLO. REV. STAT. §§ 6-1-713.5(1), 6-1-713.5(2)(b) (2018).

22 N.Y. GEN. BUS. § 899-bb(2)(a) (McKinney 2020).

23 OHIO REV. CODE ANN. § 1354.03 (West 2018).

24 *See infra* Section I.A.

Inc. v. Federal Trade Commission cases, actions brought as a result of Federal Trade Commission (FTC) investigations following significant data breaches.[25] In both of these cases, the FTC sought to enforce cybersecurity standards under its consumer protection authority to protect against deceptive or unfair business practices under the FTC Act.[26] The facts in *Wyndham* are particularly egregious, where the multinational hotel company's lax cybersecurity practices resulted in three significant data breaches over two years, resulting in more than $10 million in damages from identity theft and fraud.[27] The circumstances are less dramatic in *LabMD*, where a medical testing company suffered a data breach containing the personal information of 9,300 LabMD patients due to their billing manager having downloaded a peer-to-peer filesharing application that inadvertently exposed the company data externally.[28] In both cases, the FTC pointed to the parties' failure to employ reasonable cybersecurity measures as the reason for their respective data breaches, pointing to practices "likely to cause a substantial injury," which due to the large number of victims possible in cybersecurity incidents, may be considered "unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low."[29] The *Wyndham* and *LabMD* courts came to differing conclusions as to the FTC's claims, based in part on what should be considered reasonable cybersecurity.[30] We will revisit these cases—and how they might inform a better understanding of cybersecurity reasonableness—in Part II.

A. *The Reasonableness Standard*

Objectivity is a cornerstone of American legal theory.[31] Much of our jurisprudence depends on a principle of reasonableness as a means of developing an objective standard within a liberal society that values

---

25 FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 242–43 (3d Cir. 2015); LabMD, Inc. v. FTC, 894 F.3d 1221, 1230–31 (11th Cir. 2018).

26 15 U.S.C. § 45.

27 *Wyndham Worldwide Corp.*, 799 F.3d at 240.

28 *LabMD, Inc.*, 894 F.3d at 1224.

29 *In re* LabMD, Inc., No. 9357, 2016 WL 4128215, at *10–11 (F.T.C. July 28, 2016), *vacated*, LabMD, Inc. v. FTC, 894 F.3d 1221, 1230–31 (11th Cir. 2018).

30 Whereas the Third Circuit held that Wyndham had fair notice of what were reasonable cybersecurity practices, the Eleventh Circuit in *LabMD* held that the FTC's order was not sufficiently specific to meet fair notice standards. *See Wyndham Worldwide Corp.*, 799 F.3d at 256; *LabMD, Inc.*, 894 F.3d at 1236.

31 *See* OLIVER WENDELL HOLMES, JR., THE COMMON LAW 6-15, 38 (1945) (contrasting the ideal of objectivity with the notion of vengeance as an early, primitive basis of legal thought, noting that an advanced civilization requires the development of law based on an objective standard).

individual freedoms and interactions while protecting those individuals when those interactions result in injury.[32] Enforcing rules within such a political arrangement requires that the law should avoid favoring one party over another lest it allow individuals to unfairly leverage the power of the state over others.[33] This kind of objective measure is defined within our legal system by what is considered "reasonable behavior," based on the liberal ideal of a social contract between citizens and their government, where individuals agree to conduct themselves according to accepted standards—which may change based on time and geography—and can expect the same of their fellow citizens in return.[34]

Reasonableness, then, is a compromise between our freedom, right, or desire to act as we choose, and our right and desire for security against the harms arising out of the actions of others.[35] This concept was especially important in areas such as criminal law, where the state exercised significant power against its citizens.[36] To better account for the fallibility of individuals, including agents of the state, concepts such as reasonable doubt of guilt emerged.[37] From this understanding, common law definitions were first expressly articulated in the mid-nineteenth century in the context of negligence in British courts.[38]

---

32 Singer, *supra* note 4, at 980–81 ("Liberalism is the invitation to act in a self-interested manner, without impediment from other people, as long as what we do does not harm them. This political theory is founded on a contradiction. We want freedom to engage in the pursuit of happiness. Yet we also want security from harm. The more freedom of action we allow, the more vulnerable we are to damage inflicted by others. Thus, the contradiction is between the principle that individuals may legitimately act in their own interest to increase their wealth, power, and prestige at the expense of others and the principle that they have a duty to look out for others and to refrain from acts that hurt them. Since liberal citizens are motivated by self-interest, the only way to achieve security is to give power to the state to limit freedom of action. The contradiction between freedom of action and security therefore translates into the contradiction between individual rights and state powers. We must determine the extent to which individual freedom of action may legitimately be limited by collective coercion over the individual in the name of security." (citation omitted)).

33 *Id.*

34 *Id.* at 982–83.

35 We see this compromise arise in multiple areas of the law. *See, e.g.*, Robert M. Keenan III, Shoemaker v. Handel *and Urinalysis Drug Testing: Looking for an American Standard*, 21 GA. L. REV. 467, 469–70 (1986) (discussing the concept of reasonable suspicion in Fourth Amendment contexts and its tension with the individual privacy provided for by the Fourth Amendment and elsewhere).

36 *See, e.g.*, Anthony A. Morano, *A Reexamination of the Development of the Reasonable Doubt Rule*, 55 B.U. L. REV. 507 (1975).

37 *Id.*

38 Vaughan v. Menlove, (1837) 132 Eng. Rep. 490, 492 (C.P.) (stating that the defendant "was bound to proceed with such reasonable caution as a prudent man would have exercised under such circumstances"); Blyth v. Birmingham Waterworks Co., (1856) 156 Eng. Rep. 1047, 1049 (Exch.) ("Negligence is the omission to do something which a reasonable man, guided upon those

A significant source of the allure behind reasonableness as a standard is its ability to be modified based on current, relevant norms.[39] When a jury is asked to determine whether or not a defendant is negligent, it is assumed that they understand their community's norms and values, and how a reasonable person would see them.[40] This flexible basis for as accurate and objective a standard as possible is seen throughout tort law.[41] Similarly, the reasonable expectation test in Fourth Amendment jurisprudence is explicitly one that rests on community (or societal) norms and values.[42] Even when a dispute involves commercial entities and interests, questions of industry norms arise, as well as questions as to how they should be applied.[43]

With this flexibility comes the possibility that a standard can be unfairly manipulated and introduce the kinds of complexity that accompany the need to communicate the metes and bounds of the standard. But in this complexity of communication, there is an onus put on parties to evaluate the terms of the flexible standard, meaning that the parties must also communicate their intentions to one another. This kind of framework is not useful in all circumstances, but its flexibility is desirable when individualized and dynamic facts present themselves that strain the usefulness of a rule-based framework, which demands certainty and control of the facts and falters when those facts do not fit well into its pattern.[44]

---

considerations which ordinarily regulate the conduct of human affairs, would do, or doing something which a prudent and reasonable man would not do.").

39 *See, e.g.*, Stephen G. Gilles, *On Determining Negligence: Hand Formula Balancing, The Reasonable Person Standard, and the Jury*, 54 VAND. L. REV. 813, 833–34 (2001).

40 *Id.*

41 *See* Daniel Gilman, *Of Fruitcakes and Patriot Games*, 90 GEO. L.J. 2387, 2387 (2001) ("Myriad norms, mores, customs, and customary understandings play a complex role in the law, from informing the 'reasonable man' and 'reasonable person' standards in tort law (and elsewhere), to filling in the normal and customary practices that vary across trades in commercial law. Interesting and complex borderline cases arise as well, cases in which nonlegal standards increasingly resemble law, both formally and substantively.").

42 *See, e.g.*, William C. Heffernan, *Fourth Amendment Privacy Interests*, 92 J. CRIM. L. & CRIMINOLOGY 1, 3637 (2002) ("Harlan viewed an expectation of privacy as objectively valid only if it is one 'society is prepared to recognize as "reasonable."' Harlan's approach thus requires courts to examine society's practices—and so to look beyond the Constitution's text—in trying to discern privacy norms.").

43 *See* Jody S. Kraus, *Legal Design and the Evolution of Commercial Norms*, 26 J. LEG. STUD. 377, 410 (1997) ("[T]he same forces affecting the evolution of commercial norms will affect the evolution of norms governing any potential process that attempts to improve on commercial norms. Although these norms are not themselves commercial norms, they may also impede attempts to improve on commercial practice. To make the positive case for supplementing the incorporation strategy with alternative legal design strategies, more must be done than demonstrating that these practices leave room for improvement."); *see also infra* Section II.A.

44 *See* Pierre J. Schlag, *Rules and Standards*, 33 UCLA L. REV. 379, 405–07 (1985).

The application of a reasonableness standard is based on, but does not strictly adhere to, ordinary dictionary definitions of the term, many of which themselves rely on some rather inexact terms.[45] Second Circuit Senior Judge Jon Newman describes four contexts through which courts translate our colloquial understandings of the term for legal purposes: reasonableness as a continuum, as a balancing exercise, as a set of standards or factors within some kind of reasonable test, or simply as its own test without any explicitly defined analysis or factors.[46]

The legal fiction of the reasonable person, then, was created as a stand-in for what might be characterized as the ordinary, the commonplace, or the characteristics of someone randomly selected from the "ordinary," "but still commonplace" people from the great middle of society.[47] This is not necessarily representative solely of a normative societal ideal, but rather meant as a mix of both common and sensible, an assumption that those from this "ordinary mass" are those without extreme sensibilities, ambitions, or prejudices, but are instead generally law-abiding, taxpaying citizens whose opinions on justice are worthy of a court's respect.[48] From these origins, it becomes easier to see the emergence of a reasonable person standard as, for example, a basis for negligence liability, where one applies the "reasonable caution" of a "prudent man," although one can also see arguments that averageness and "prudence" are not necessarily cut from the same cloth.[49]

A reasonableness standard can therefore give societies the wherewithal to adjust their legal systems to fit contemporary values in ways that do not necessarily require the employment of legislative or regulatory machinery. It is important to note here that a common law application of reasonableness standards does not preclude legislation or regulation.[50] In fact, these areas of law can often work in tandem to

---

45 *See* Jon O. Newman, *On Reasonableness: The Many Meanings of Law's Most Ubiquitous Concept*, 21 J. APP. PRAC. & PROCESS 1, 3 (2021) (illustrating how colloquial understandings of reasonableness can take various forms, some of them inconsistent with one another, and often inexact in their definition).

46 *Id.*

47 WALTER BAGEHOT, THE ENGLISH CONSTITUTION 325–26 (1873).

48 *Id.* at 326 ("The English constitution in its palpable form is this—the mass of the people yield obedience to a select few; and when you see this select few, you perceive that though not of the lowest class, nor of an unrespectable class, they are yet of a heavy sensible class—the last people in the world to whom, if they were drawn up in a row, an immense nation would ever give an exclusive preference.").

49 Vaughan v. Menlove (1837) 132 Eng. Rep. 490, 492 (C.P.).

50 In fact, states can enact legislation that adopts common law reasonableness standards or defines its own standard, which can sometimes create additional work for courts navigating interweaving standards. *See, e.g.*, Carlos E. González, *The Logic of Legal Conflict: The Perplexing Combination of Formalism and Anti-Formalism in Adjudication of Conflicting Legal Norms*, 80 OR. L. REV. 447, 554–57 (2001).

address existing social and economic issues. When, for example, the United States and United Kingdom began to experience negative effects brought about by the relatively rapid changes to the manufacture and sale of products that accompanied the Industrial Revolution, the notion of what was and was not reasonable manufacturer or seller behavior began to change in ways meant to address these effects. Through the early- to mid-nineteenth century, the longstanding common law rule regarding a defective product was well articulated by the English Court of Exchequer in *Winterbottom v. Wright*, which required privity of contract in order to recover in negligence for harm associated with a defective product.[51] But in 1852, a New York court, considering a case where mislabeled poison sold through multiple intermediaries injured its ultimate purchaser, held that the privity rule of *Winterbottom* did not apply when the product in question was "imminently dangerous to human life."[52] These exceptions to the privity rule expanded over the subsequent decades to become products liability law, and our statutory and regulatory frameworks followed this consumer safety trend.[53]

In the same way we saw the negative effects of changing manufacturing and sales methods and standards, we are now experiencing the resulting cybersecurity failures within our increasingly technology-dependent society. In the early days of digital computing, our concepts of injury and harm were based in large part on the very limited use—and use cases—of these technologies.[54] The technical details behind these technologies were opaque or unknowable to most people, making it difficult for juries, courts, lawmakers, and regulators to apply rules that preexisted these machines. As one might expect the law that emerged out of these early days reflected this natural ambivalence. Unfortunately, however, we are experiencing a kind of hangover from the rules meant to address a simpler time. We developed a very narrow understanding of the kinds of harm that can come from cybersecurity failures. Now that so much depends on the security and reliability of computers and networks,

---

51 *See generally* Winterbottom v. Wright, (1842) 152 Eng. Rep. 402 (Exch.).

52 Thomas v. Winchester, 6 N.Y. 397, 408 (1852).

53 *See, e.g.*, Kyle Graham, *Strict Products Liability at 50: Four Histories*, 98 MARQ. L. REV. 555 (2014); *see also infra* Section II.C.

54 This is a significant source of the problem when considering liability for faulty software. As technological innovations continue to emerge, courts can have difficulties applying existing legal regimes to circumstances that could not have been anticipated at the time of a law's original drafting. *See, e.g.*, Jake Goldenfein, Deirdre K. Mulligan, Helen Nissenbaum, & Wendy Ju, *Through the Handoff Lens: Competing Visions of Autonomous Futures*, 35 BERKELEY TECH. L.J. 835, 871–74 (2020) (discussing the liability challenges faced by the advent and growth of autonomous vehicles and the novel fact patterns that can emerge from them).

and the body of technical knowledge has grown to meet these needs, we should adjust our idea of reasonable cybersecurity accordingly.[55]

B. *The Difficulties of Cybersecurity Liability*

Efforts to apply a reasonableness standard to cybersecurity have encountered a series of obstacles of varying significance since this new species of technological problem arose with the advent of computer hardware, software, and networking.[56] Perhaps first among these obstacles is our legal system's overall reluctance to find civil liability for cybersecurity failures.[57] Getting through the courthouse doors can be difficult if a court will not recognize your injury as sufficient to support standing.[58] A tort claim may be precluded by the fact that a consumer contract waiving liability was agreed to when the software or hardware was purchased.[59] And even if a tort claim might be recognized, the economic loss doctrine may limit or prevent recovery depending on the jurisdiction.[60]

There has also been a definitional problem: a lack of a widely-accepted definition for insufficiently secure software has made claims as

---

55 *See infra* Part III.

56 The infamous 1988 Morris Worm was perhaps the first large-scale cybersecurity incident to attract significant attention. Its rapid spread and significant effects were early signs of what a highly connected technological infrastructure meant for reliability, interdependence, and security. *See* Scott Schackelford, *30 Years Ago, the World's First Cyberattack Set the Stage for Modern Cybersecurity Challenges*, CONVERSATION (Nov. 1, 2018, 10:16 AM), https://theconversation.com/30-years-ago-the-worlds-first-cyberattack-set-the-stage-for-modern-cybersecurity-challenges-105449 [https://perma.cc/57EH-HU56].

57 *See, e.g.*, Vincent R. Johnson, *The Boundary-Line Function of the Economic Loss Rule*, 66 WASH. & LEE L. REV. 523 (2009); David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935 (2016); 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); Frances E. Zollers, Andrew McMullin, Sandra N. Hurd & Peter Shears, *No More Soft Landings for Software: Liability for Defects in an Industry That Has Come of Age*, 21 SANTA CLARA COMPUT. & HIGH TECH. L.J. 745 (2005); Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425 (2008); Michael Rustad & Lori E. Eisenschmidt, *The Commercial Law of Internet Security*, 10 HIGH TECH. L.J. 213 (1995).

58 *See* Justin (Gus) Hurwitz, *Cyberensuring Security*, 49 CONN. L. REV. 1495, 1514 & n.37 (2017).

59 *See* Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1536–37 (2013).

60 *See* Opderbeck, *supra* note 57.

to reasonable cybersecurity difficult to establish.[61] That is to say, courts and claimants will often use terms like "insecure software," but such terms are not necessarily defined in a way that courts can use to define reasonableness in this context.[62] Finally, there is a strong protectionist strain throughout American technology law and policy arguments that is based on the fear that any accountability framework that might stifle innovation is problematic, and argues that any such liability arrangements for cybersecurity or other software flaws should first take into account the greater public good technology manufacturers provide.[63]

This legal landscape has left questions of cybersecurity accountability in a confused and conflicted state. Products liability, for example, which might seem an appropriate framework to address the problem of insecure software-related products, has proven nearly impossible to apply in this context for a host of historical reasons.[64] And one might think that questions regarding the applicability of contracts to indemnify software manufacturers against future claims would have faced limiting principles or even outright rejection by courts given their arguably adhesive nature. However, that history has also proven more complicated and has favored manufacturers.[65]

One could argue that these kinds of obstacles are symptoms of the natural lag time between existing legal frameworks and the rapid growth of new technologies, but scholars have pointed to the rising tide of cybersecurity problems and have been recommending alternative means to address this increasingly difficult issue.[66]

---

61 Marian K. Riedy & Bartlomiej Hanus, *It Is Just Unfair Using Trade Laws to "Out" Security Software Vulnerabilities*, 48 LOY. U. CHI. L.J. 1099, 1130–31 (2017) ("What, specifically, the software vendor has done that is 'unfair' when it licenses insecure software is another issue. Just as a company is generally required to take 'reasonable' security measures, a security-software vendor could be required to license 'reasonably secure' software. Pursuant to such a standard, a security-software vendor would be subject to FTC action should a substantial risk of harm result if its software is not 'reasonably secure.' Defining 'reasonable security measures' is no simple task, however, and attempting to define 'reasonably secure software' is probably *even more* difficult.").

62 *Id.*

63 The protection of the American technology industry has a history that goes back to the post-war years and the explosion of technology companies that followed the inventions of the transistor and semiconductor. *See* MARGARET O'MARA, THE CODE: SILICON VALLEY AND THE REMAKING OF AMERICA 29–33 (2019).

64 *See* Sales, *supra* note 59, at 1533–36.

65 *See* Russell Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. CHI. L. REV. 1203, 1265 (2003); David Horton, *Indescendibility*, 102 CAL. L. REV. 543, 597–98 (2014).

66 *See, e.g.*, Scott, *supra* note 57; Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J 1553 (2005); Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L & PUB. POL'Y 283 (2006); Hurwitz, *supra* note 58; Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255 (2005).

II. FINDING RELEVANT REASONABLENESS STANDARDS

As discussed above, the concept of reasonableness as a standard plays a role in multiple areas of U.S. law. While there are valuable lessons to be gleaned from each of these areas, this Article will concentrate on reasonableness and related standards from a select set of specific areas, concentrating especially on the setting and enforcing regulatory rules, negligence, and negligence per se. This Article explores these areas because their subject matters and fact patterns are generally closer to the problems described in this Article, and thus they hold the most promise for the development of a reasonableness standard in cybersecurity law. This is not meant to be an exhaustive list of possibilities, however, and follow-on work may develop the theory further.

A. *Common Law Standards of Reasonableness*

1. Reasonableness in Negligence Cases

Law students often get their first lesson in reasonableness when they encounter the "reasonable person" standard in torts.[67] As part of the introduction to the concept, students learn that the reasonableness standard is meant to be objective, deciding questions of negligence through a uniform measure that compares actions with the conduct of a hypothetical reasonable person, removing personal and subjective attributes and characteristics from the equation.[68] This concept is an important facet of tort law generally, which means to set up a fair process for attaching liability in as objective a manner as possible.[69]

To remain objective, the reasonableness standard must be seen within the context of customary practice. What is, and is not, socially acceptable within the framing of the case being considered will steer a court's thinking on reasonableness. In medical malpractice cases, for example, courts will look to a standard of reasonable medical care, an objective metric based on current thinking in the appropriate medical

---

67 *See, e.g.*, Palsgraf v. Long Island R.R. Co., 162 N.E. 99, 99–100 (N.Y. 1928); 57A AM. JUR. 2D NEGLIGENCE § 130 (2024) ("The phrasing of the standard of care in negligence cases in terms of the 'reasonable person' is firmly implanted in the American law of negligence. The standard of care is often stated as the 'reasonably prudent person standard,' or some variation thereof, or in other words, what a reasonable person of ordinary prudence would have done in the same or similar circumstances.") (footnote omitted); RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 3 cmt. a (AM. L. INST. 2010).

68 *See* HOLMES, *supra* note 31, at 107–09.

69 *See* ARTHUR RIPSTEIN, EQUALITY, RESPONSIBILITY, AND THE LAW 84–87 (1999).

field that is supported by expert testimony.[70] Similarly, courts considering cases of negligence within the context of a particular industry may look to current industry customs relating to the injury at hand, sometimes even asserting that those customs themselves are negligent.[71]

Relevant to this Article, this latter rule has not necessarily always been the final deciding factor in attaching liability due to negligence. If evidence shows that a firm's actions, while within the boundaries of industry custom, are still negligent due to technological advances, better available designs, or even what is considered socially acceptable behavior—itself a kind of reasonableness—a court may still hold a defendant liable for those actions. Perhaps the most well-known case describing this standard is that of *The T.J. Hooper*.[72] In that case, Judge Hand held that a tugboat company's failure to carry a radio on board could be negligent, despite the fact that industry custom at the time did not require radios on tugboats.[73] Judge Hand observed that,

> [I]n most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices. It never may set its own tests, however persuasive be its usages. Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission.[74]

Ultimately, Judge Hand ruled that while an industry custom is relevant to whether a defendant was negligent, a court could find that a defendant who complied with a custom was nevertheless negligent.[75]

Similarly, in *Texas & Pacific Railway Company v. Behymer*, railroad companies had, by industry custom, required their employees stand on the slippery tops of railroad cars to remove ice without first ensuring that the cars did not move while they performed this duty.[76] Justice Holmes

---

70 *See, e.g.*, Maurer v. Trustees of Univ. of Penn., 614 A.2d 754, 757–58 (Pa. Super. Ct. 1992); Tarasoff v. Regents of Univ. of Cal., 551 P.2d 334, 343–45 (Cal. 1976).

71 Generally, an actor's failure to adhere to current industry customs and practices is a strong indicator that the defendant acted negligently. *See* DAN B. DOBBS, THE LAW OF TORTS § 9 16 (2000) (describing tort liability as based on deviation from acceptable standards); *id.* § 164, at 397; *cf.* T.J. Hooper, 60 F.2d 737, 740 (2d Cir. 1932) (holding that a tug company's failure to carry a radio on board could have been negligent, even though, by custom, those vessels did not often carry radios at the time and observing that "a whole calling may have unduly lagged in the adoption of new and available devices"). Ultimately, Judge Hand ruled that while an industry custom is relevant to whether a defendant was negligent, a court could find that a defendant who complied with a custom was nevertheless negligent. *T.J. Hooper*, 60 F.2d at 740.

72 *T.J. Hooper*, 60 F.2d at 740.

73 *Id.*

74 *Id.*

75 *Id.*

76 189 U.S. 468, 469–70 (1903).

observed rather tartly that "[w]hat usually is done may be evidence of what ought to be done, but what ought to be done is fixed by a standard of reasonable prudence, whether it usually is complied with or not."[77] Holmes allowed that a "certain amount of bumping and jerking is to be expected on freight trains," yet that those circumstances "can be avoided, if necessary" when it is "obviously dangerous to those known to be on top of the cars."[78]

The fact patterns of *T.J. Hooper* and *Behymer* are perhaps less likely to be found in modern circumstances due to better regulatory standards and enforcement and, in no small part, the decades of case law that have improved industry practices and helped establish more stringent consumer-related social acceptability norms over that time.[79] Industries, realizing the commercial and legal advantages available to companies that make reasonable and sustained efforts to avoid customer or worker harm, have made significant efforts to adopt customs that avoid the "is done" versus "ought to be done" issues raised by Justice Holmes.[80]

But there is a principle of common sense that must remain in the background of such decisions regarding what is and is not reasonable. This is not the same as what might be rational under the circumstances. It may have been a rational business decision at the time for the owners of the *T.J. Hooper* not to install a radio aboard their tugboats or for the Texas and Pacific Railway Company not to take steps to avoid injuries to their employees, but in both of these instances courts were willing to look beyond what was argued as business prudence or adherence to industry customs and practices, to "what ought to be done" under a "standard of reasonable prudence"[81] in order to correct standard business practices that are "too slack."[82]

This reasonableness concept has also played an important and relevant role in the analysis of liability and professional standards of care. Medical malpractice actions, for example, have required plaintiffs show professional negligence on the part of the defendant(s), originally a reasonableness standard based on a professional standard of care, later revised by cases from the 1960s through the 1980s to one that evaluates

---

77 *Id.* at 470.

78 *Id.*

79 This is perhaps most visible in the significant changes in industry practices caused by environmental regulation. *See* Robert F. Blomquist, *Government's Role Regarding Industrial Pollution Prevention in the United States*, 29 GA. L. REV. 349, 354–83 (1995) (describing the emergence of pollution prevention as a regulatory paradigm in the 1960s and 1970s).

80 *See, e.g.*, Clayton P. Gillette & James E. Krier, *Risk, Courts, and Agencies*, 138 U. PA. L. REV. 1027, 1038–39 (1990).

81 *Behymer*, 189 U.S. at 469.

82 T.J. Hooper, 60 F.2d 737, 740 (2d Cir. 1932).

medical treatment as reasonable if "supported by reputable, respectable, and reasonable medical experts."[83] These standards often look to what is (or what should be) foreseeable to a competent professional in the field, whose ordinary skill and competence in delivering services should include the ability to foresee both potential injuries as well as potential victims.[84]

As illustrated above, what a court considers reasonable will naturally change over time. But since the mid-twentieth century, this standard has been subject to significant changes that originate with the movement toward economic reasoning in tort law that have confused the standard in the attempt to clarify it.[85] Tort law, economists say, should not concern itself with the total social costs of a case, but should look instead to marginal social costs.[86] That is, if someone stands to gain more than the average person by taking additional care, they will rationally do so. The reverse also holds.[87] Thus, rather than trying to apply an objective standard of reasonableness, courts should hold defendants with greater capacity (and thus higher marginal gain) to a higher standard of care than those with lesser capacity. This approach appears to align with the

---

83 Furey v. Thomas Jefferson Univ. Hosp., 472 A.2d 1083, 1089 (Pa. Super. 1984) (addressing the "two schools of thought" doctrine, where there is more than one method of accepted treatment for a patient's disease or injury and observing the reasonableness rule is to be applied when "medical authority is divided").

84 Perhaps the most well-known articulation of this reasonableness standard can be found in *Tarasoff v. Regents of the Univ. of Cal.*, 551 P.2d 334 (Cal. 1976), where the California Supreme Court heard a case where a therapist's patient murdered the plaintiffs' daughter after that patient had told the therapist of his violent intentions. The court held that

> once a therapist does in fact determine, or under applicable professional standards reasonably should have determined, that a patient poses a serious danger of violence to others, he bears a duty to exercise reasonable care to protect the foreseeable victim of that danger. While the discharge of this duty of due care will necessarily vary with the facts of each case, in each instance the adequacy of the therapist's conduct must be measured against the traditional negligence standard of the rendition of reasonable care under the circumstances.

Id. at 345.

85 *See, e.g.*, Gregory C. Keating, *Reasonableness and Rationality in Negligence Theory*, 48 STAN. L. REV. 311 (1996); Christopher Brett Jaeger, *The Empirical Reasonable Person*, 72 ALA. L. REV. 887 (2021); David W. Barnes & Rosemary McCool, *Reasonable Care in Tort Law: The Duty to Take Corrective Precautions*, 36 ARIZ. L. REV. 357 (1994).

86 *See, e.g.*, David Crump, *Evidence, Economics, and Ethics: What Information Should Jurors Be Given to Determine the Amount of a Punitive-Damage Award?*, 57 MD. L. REV. 174, 192–93 (1998).

87 *See, e.g.*, WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF TORT LAW 123–24 (1987) ("A potential injurer who was very clumsy would have a low [efficient level of care] because his investment in care would be relatively unproductive and his marginal cost of care would be relatively high; one who had exceptionally quick reflexes would be highly productive and his marginal cost would be low, so he would have a high [efficient level of care].").

longstanding approach to reasonableness that holds select defendants to lower or higher standards of care, depending on their circumstances.[88]

2. Reasonableness in Products Liability Cases

Products liability has had a rather turbulent history in U.S. jurisprudence. We have gone from what was essentially a system based on caveat emptor in the early nineteenth century, to broader acceptance of the concept of implied warranties (with many exceptions) around the turn of the twentieth century, to the rejection of manufacturers' privity defenses and the beginning of modern products liability law in the mid-twentieth century.[89] Out of this rapid set of changes emerged strict products liability, based on the reasoning that negligence law alone was not enough to deal with the problem of defective products.[90] And while strict products liability and cybersecurity is a highly worthwhile topic to pursue, this Article will limit this analysis to negligence liability regarding products and its relationship to reasonableness.

Products liability cases arise when manufacturers produce or sell a defective product and are therefore "subject to liability for harm to

---

88 *See, e.g.*, DAN B. DOBBS, PAUL T. HAYDEN & ELLEN M. BUBLICK, THE LAW OF TORTS §§ 129 284 (2d ed. 2024) (describing instances of lesser or greater standards of care for certain circumstances).

89 Until the mid-twentieth century, products liability claims were often blocked by the doctrine that prohibited actions against remote manufacturers with whom plaintiffs had no privity of contract. To hold otherwise, went the doctrine, would hamper the growth of American industry, because if a manufacturer "owes a duty to the whole world" that their products are free from hidden defects, "it is difficult to measure the extent of his responsibility, and no prudent man would engage in such occupations upon such conditions." Curtain v. Somerset, 21 A. 244, 245 (Pa. 1891). This began to change with the case of *MacPherson v. Buick Motor Co.*, 111 N.E. 1050 (N.Y. 1916). There, the New York Court of Appeals held that the imminent danger exception to the privity requirement, usually limited to highly dangerous products only, was extended to other products where "the nature of a thing is such that it is reasonably certain to place life and limb in peril when negligently made." Manufacturers of these products, irrespective of privity of contract, are "under a duty to make it carefully." *Id.* at 1053. Courts continued to expand the doctrine, and in 1960, the New Jersey Supreme Court held a defendant manufacturer liable even in the face of a lack of privity as well as disclaimers of responsibility. Henningsen v. Bloomfield Motors, Inc., 161 A.2d 69 (N.J. 1960). The court was especially critical of the disclaimer and liability limitation clauses in the fine print of the form presented by the defendant, holding that they were based on the "gross inequality of bargaining position" of the consumer, and were therefore unconscionable contracts of adhesion. *Id.* at 87.

90 The beginning of strict products liability is often marked by three events. *See Henningsen*, 161 A.2d at 77; Greenman v. Yuba Power Products, Inc., 377 P.2d 897, 900 (Cal. 1963); William L. Prosser, *The Assault upon the Citadel (Strict Liability to the Consumer)*, 69 YALE L.J. 1099, 1110–12 (1960).

persons or property caused by the defect."[91] A defective product, in turn, is defined as a product

> when, at the time of sale or distribution, it contains a manufacturing defect, is defective in design, or is defective because of inadequate instructions or warnings. A product:
>
> (a) contains a manufacturing defect when the product departs from its intended design even though all possible care was exercised in the preparation and marketing of the product;
>
> (b) is 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 by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the alternative design renders the product not reasonably safe;
>
> (c) is defective because of inadequate instructions or warnings when the foreseeable risks of harm posed by the product could have been reduced or avoided by the provision of reasonable instructions or warnings by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the instructions or warnings renders the product not reasonably safe.[92]

As discussed below,[93] theories of negligence are based on principles of reasonableness, balance, and often a utilitarian sense of optimal solutions. One can see these same principles at work in products liability cases, as well, especially in liability for faulty design. Specifically, in order for a design to be considered defective, a product must be shown to be "not reasonably safe," which requires that the manufacturer failed to adopt a "reasonable alternative design."[94] The comments even note that design defectiveness is judged by "a reasonableness ('risk-utility' balancing) test" as seen by "a reasonable person . . . used in administering the traditional reasonableness standard in negligence."[95]

A products liability case based on negligence depends on the question of whether the defendant's conduct was reasonable in view of the foreseeable risk of injury.[96] One point worth briefly noting here is the

---

91 RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 1 (AM. L. INST. 1998).

92 *Id.* § 2.

93 *See infra* Section II.B.

94 RESTATEMENT (SECOND) OF TORTS: PROD. LIAB. § 2(b) (AM. L. INST. 1998).

95 *Id.* cmt. d.

96 *See, e.g.*, Hakim v. Safariland, LLC, 410 F. Supp. 3d 862 (N.D. Ill. 2019); Certain Underwriters at Lloyd's v. S. Pride Trucking, Inc., 331 F. Supp. 3d 956 (D. Neb. 2018); Stahlecker v. Ford Motor Co., 667 N.W.2d 244 (Neb. 2003).

existence of theories that hold manufacturers or sellers of products that are not reasonably safe when used in a reasonable or customary manner negligent as a matter of law.[97] This Article will return to this point in a subsequent section.[98]

Because of the existence of multiple theories of product liability, it is important to distinguish how a products liability negligence case is distinguished from other theories. Products liability claims based on breach of warranty or strict liability theories have somewhat eclipsed negligence claims, as the former theories do not require proof of specific negligence by the manufacturer.[99] Note, however, that a court's determination that a manufacturer is strictly liable for a defective product is completely independent of the question of whether or not a defect was caused by the manufacturer's negligence.[100] Products liability claims can be based on both negligence and strict liability theories.[101] Some jurisdictions have codified strict liability rules that remove any distinction between the three products liability theories.[102]

3. Strict Products Liability

Before jumping into theories of negligence in products liability claims, however, there is a particularly relevant aspect of strict products liability cases that allege design defects. As defined by the Restatement (Third) of Torts, a product

> is 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 by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission

---

97 *See* Hicks v. Vulcan Engineering Co., 749 So. 2d 417, 422 (Al. 1999) ("[A] manufacturer, supplier, or seller who markets a product not reasonably safe when applied to its intended use in the usual and customary manner, is negligent as a matter of law. In other words, the fault or negligence of the defendant is that he has conducted himself in a negligent manner by placing on the market a product that causes personal injuries or property damage when put to its intended use. As long as there is a causal relationship between the defendant's conduct and the defective product, liability may attach, because an unreasonable risk of harm has been created.").

98 *See infra* Section II.E.

99 *See, e.g.*, Est. of Hicks v. Dana Cos., 984 A.2d 943 (Pa. Super. Ct. 2009) (providing that negligence concepts do not have a role in a strict liability case).

100 *See* Godoy *ex rel.* Gramling v. E.I. du Pont de Nemours & Co., 2009 WI 78, 8 n.7, 319 Wis.2d 91, 106 n.7, 768 N.W.2d 674, 681 n.7 (Wis. 2009).

101 *See, e.g.*, Richard Ausness, *Product Liability's Parallel Universe: Fault-Based Liability Theories and Modern Products Liability Law*, 74 BROOK. L. REV. 635, 635 (2009).

102 *See, e.g.*, Allard v. Liberty Oil Equip. Co., 756 A.2d 237 (Conn. 2000); Tirrell v. Navistar Int'l, Inc., 591 A.2d 643 (N.J. Super. Ct. App. Div. 1991); Wash. Water Power Co. v. Graybar Elec. Co., 774 P.2d 1199 (Wash. 1989) (en banc), *amended on other grounds by* 779 P.2d 697.

> of the alternative design renders the product not reasonably safe . . . .[103]

The requirement imposed on plaintiffs bringing such a claim in strict products liability to prove the existence of a "reasonable alternative design" provides a basis for a strong argument that these claims sound in negligence, not in strict liability.[104] Compare this requirement with the Restatement's definition of manufacturing defect claims:

> A product[] contains a manufacturing defect when the product departs from its intended design even though all possible care was exercised in the preparation and marketing of the product . . . .[105]

Under this definition, the Restatement notes that the "superior standard" for analyzing manufacturing defects is strict liability.[106] Reasonableness of design in these contexts requires an independent assessment of design tradeoffs, possibly applying the sort of "risk-utility balancing" test found in the Hand formula.[107] Compare this standard with that found in the Restatement (Second), which states that products liability cases should apply a consumer expectation test. That is, a product should be seen as defective if it does not meet a reasonable consumer's expectations of safety.[108]

The tension surrounding this difference in standards is based largely in the concern that harmful product defects might be somehow excused in the name of economic efficiency.[109] Applying this balancing test puts consumers and manufacturers in equalized initial positions, then weighs the costs and benefits in a clinical manner that, bluntly, assumes that a nonnegligible percentage of products are intentionally designed to be

---

103 RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2(b) (AM. L. INST. 1998).

104 The introduction to the Restatement (Third) of Torts notes that "Section 2(b) generated considerable controversy. It calls for proof of a reasonable alternative design in order to sustain an action for defective design[,]" but cautions that the Restatement "must be read as a whole. Overzealous advocates may seek to focus the attention of courts on § 2(b) alone. Users of this Restatement are cautioned against such fragmented reading." *Id.* intro.

105 *Id.* § 2(a).

106 *Id.* § 2 cmt. a.

107 United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947) (expressing the cost-benefit balancing concept in algebraic terms, as negligence being implied if B < PL, where B is the burden or cost of avoiding accidental loss, P is the increase in probability of loss if B is not undertaken, and L is the probable magnitude or cost of such loss).

108 RESTATEMENT (SECOND) OF TORTS § 402A (AM. L. INST. 1965).

109 *See, e.g.*, Paul A. LaBel, *Intent and Recklessness as Bases of Products Liability: One Step Back, Two Steps Forward*, 32 ALA. L. REV. 31, 67 (1980) ("Another of the costs that does not appear in the corporate weighing of costs and benefits of a particular product design or production process is the sense of outrage, frustration, and demoralization that accompanies the realization that the lives or physical well-being of a certain number of people have been written off by a manufacturer in pursuit of an economically efficient allocation of resources." (footnote omitted)).

only as safe or reliable as the market will bear—a deliberate decision to weigh injury against manufacturer profit.[110] Even in the cold light of this calculation, it is possible that reasonableness in cases involving cybersecurity vulnerabilities in a technology product's design could give greater weight to the consumer, as they are often in a far poorer position than the software designers to identify and minimize the risk of harm from those products.[111]

4. Products Liability and Negligence

In contrast to strict products liability, the focus of most products liability negligence claims is largely based on questions of whether the defendant's conduct was reasonable—whether they deviated from relevant accepted standards of conduct.[112] That is, where strict products liability cases focus on the reasonableness of the product, products liability negligence cases focus on the reasonableness of the manufacturer or seller.[113] Some jurisdictions describe this as the difference between a focus on whether a product is defective and whether the manufacturer's actions fell below the standard of reasonable care.[114] This means that plaintiffs in negligence cases must show that the defendant failed to exercise due care in their conduct.

The usual elements of a negligence case apply in a products liability action based on a theory of manufacturer or seller negligence. A plaintiff must show that the defendant owed the plaintiff a duty of care, that they breached this duty, and that the breach was the cause in fact of harm to

---

110 *See, e.g.*, Thomas A. Cowan, *Some Policy Bases of Products Liability*, 17 STAN. L. REV. 1077, 1086–87 (1965).

111 *See* discussion *infra* Section III.A.

112 *See, e.g.*, Hollinger v. Shoppers Paradise of N.J., Inc., 340 A.2d 687 (N.J. Super. Ct. Law Div. 1975), *aff'd*, 361 A.2d 578 (N.J. Super. Ct. App. Div. 1976).

113 *See, e.g.*, Chase Manhattan Bank v. T & N PLC, 905 F. Supp. 107, 122 (S.D.N.Y. 1995) (distinguishing strict liability and negligence in that strict liability focuses on product, whereas negligence focuses on conduct of manufacturer); Voss v. Black & Decker Mfg. Co., 450 N.E.2d 204, 207 (N.Y. 1983) (differentiating strict products liability for design defect because the plaintiff is not required to prove that the manufacturer acted unreasonably in designing the product). *But see* Keith Miller, *Design Defect Litigation in Iowa: The Myths of Strict Liability*, 40 DRAKE L. REV. 465, 480 (1991) (doubting whether courts cause "anything other than confusion" when they apply both strict liability and negligence to design defect cases).

114 *See, e.g.*, Certain Underwriters at Lloyd's v. S. Pride Trucking, Inc., 331 F. Supp. 3d 956 (D. Neb. 2018); Ostendorf v. Clark Equip. Co., 122 S.W.3d 530 (Ky. 2003); Martin v. Survivair Respirators, Inc., 298 S.W.3d 23 (Mo. Ct. App. E.D. 2009); Freeman v. Hoffman-La Roche, Inc., 618 N.W.2d 827 (Neb. 2000); Green v. Smith & Nephew AHP, Inc., 2001 WI 109, 245 Wis.2d 772, 629 N.W.2d 727 (Wis. 2001).

the plaintiff.[115] Here, the standard of care is that owed by a reasonable person in similar circumstances.[116] In cases of negligent product design claims, this means the plaintiff must show that the defendant failed to use reasonable care in designing the product, and that that failure resulted in a defective product.[117]

The standard of care in products liability actions based on negligence may be codified as statutes or regulations.[118] Such statutes and regulations may adjust the standard of care to be applied. When required by statute, the reasonable person standard of care may be replaced by a specific rule as defined in the statute.[119] For example, a statute may require both a reasonable degree of care and skill or specify a duty to warn.[120] Courts recognize violations of such statutory requirements as satisfying the breach of a duty of care element for negligence causes of action.[121] Advancing a reasonableness standard even further upon manufacturers, statutes may state that, "[i]f unreasonable risk[s of harm from] . . . a product cannot be [fixed] through [an] improved design, [manufacturing,] or warnings," a court may require the manufacturer "to take other[] reasonable action[s] to" address the unreasonable risks of harm from their product.[122]

Another relevant aspect to products liability negligence and reasonableness is a manufacturer's duty to warn that arises at the time of sale. Specifically, this duty is created when

> (a) One engaged in the business of selling or otherwise distributing products is subject to liability for harm to persons or property caused

---

115 *See, e.g.*, Williams v. Johnson & Johnson, 581 F. Supp. 3d 363 (D.R.I. 2022); Davis v. Cessna Aircraft Corp., 893 P.2d 26 (Ariz. Ct. App. 1994); Calles v. Scripto-Tokai Corp., 864 N.E.2d 249 (Ill. 2007); Gourdine v. Crews, 955 A.2d 769 (Md. 2008); Muilenberg v. Upjohn Co., 320 N.W.2d 358 (Mich. Ct. App. 1982); Toliver v. Gen. Motors Corp., 482 So. 2d 213 (Miss. 1985); Palmer v. Nan King Rest., Inc., 798 A.2d 583 (N.H. 2002); Residential Bd. of Managers of W. 52nd St. Condo. v. El-Ad 52 LLC, 140 A.D.3d 536, (N.Y. App. Div. 2016); McCollum v. Grove Mfg. Co., 293 S.E.2d 632 (N.C. Ct. App. 1982), *aff'd*, 300 S.E.2d 374 (1983); Dewayne Rogers Logging, Inc. v. Propac Indus., 299 S.W.3d 374 (Tex. App. 2009); Blank v. Garff Enters. Inc., 2021 UT App 6, 482 P.3d 258.

116 *See, e.g.*, *Davis*, 893 P.2d at 32 (explaining the rationale behind reasonable actions to include context that takes into consideration "minimal expectations" of similarly situated persons).

117 *See, e.g.*, Meidinger v. Zoetis, Inc., 588 F. Supp. 3d 947, 951–52 (D.N.D. 2022).

118 *See, e.g.*, Anderson v. Robinson, 174 S.E.2d 45 (N.C. Ct. App. 1970); Dougherty v. Santa Fe Marine, Inc., 698 F.2d 232 (5th Cir. 1983) (applying Louisiana law); Brogley v. Chambersburg Eng'g Co., 452 A.2d 743 (Pa. Super. Ct. 1982).

119 *See, e.g.*, Ross Lab'ys., v. Thies, 725 P.2d 1076 (Alaska 1986).

120 *See, e.g.*, Webb v. Sandoz Chem. Works, 69 S.E.2d 689 (Ga. Ct. App. 1952); Wolfe v. Great Atl. & Pac. Tea Co., 56 N.E.2d 230 (Ohio 1944).

121 *See, e.g.*, D.L. by Friederichs v. Huebner, 329 N.W.2d 890 (Wis. 1983), *superseded by statute*, WIS. STAT. § 895.047 (2011), *as recognized in* Murphy v. Columbus McKinnon Corp., 2022 WI 109, ¶ 2, 405 Wis. 2d 157, 164, 982 N.W.2d 898, 902.

122 *See, e.g.*, Allen v. Am. Cyanamid, 527 F. Supp. 3d 982 (E.D. Wis. 2021).

> by the seller's failure to provide a warning after the time of sale or distribution of a product if a reasonable person in the seller's position would provide such a warning.
>
> (b) A reasonable person in the seller's position would provide a warning after the time of sale if:
>
> (1) the seller knows or reasonably should know that the product poses a substantial risk of harm to persons or property; and
>
> (2) those to whom a warning might be provided can be identified and can reasonably be assumed to be unaware of the risk of harm; and
>
> (3) a warning can be effectively communicated to and acted on by those to whom a warning might be provided; and
>
> (4) the risk of harm is sufficiently great to justify the burden of providing a warning.[123]

Some jurisdictions do not recognize this duty in products liability cases when it would create a perpetual duty for manufacturers to rebuild or refit all existing products whenever new safety measures or devices are developed.[124] This exception will be an important question regarding the reasonableness of a software manufacturer's duties to update older versions of its products.

The concepts of strict liability and negligence have been combined somewhat by the Restatement (Third) of Torts, which has introduced the negligence principles of reasonableness and foreseeability into strict liability language regarding failure to warn, stating that a product

> is defective because of inadequate instructions or warnings when the foreseeable risks of harm posed by the product could have been reduced or avoided by the provision of reasonable instructions or warnings by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the instructions or warnings renders the product not reasonably safe.[125]

An adequate failure to warn, therefore, may include analysis of whether the notice was reasonably provided in a way that warns of foreseeable risks, a concept that could be applied to software products, especially when they are repackaged and sold by third parties.

Despite an apparent suitability of products liability claims for cybersecurity failures, they have proven difficult to bring in cases

---

123 RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 10 (AM. L. INST. 1998).

124 *See, e.g.*, DeSantis v. Frick Co., 745 A.2d 624 (Pa. Super. Ct. 1999) (providing no post-sale duty to warn about a device that would prevent damage to industrial freezers).

125 RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2(c) (AM. L. INST. 1998).

involving software products.[126] These difficulties arise from a number of sources, the details of which this Article will discuss in a subsequent section.[127] For the time being, however, please apply this Article's overarching caveat regarding the search for reasonable cybersecurity: the scope of this Article is to first find a convincing basis for reasonableness when considering liability and accountability for cybersecurity failures, even if the resulting framework might meet resistance by courts applying rules or doctrines that have not yet caught up with contemporary technology realities.[128]

5. Reasonableness in Premises Liability Cases

Cases involving a reasonableness standard in premises liability contexts are perhaps an unusual place to start looking for ways to derive a reasonable cybersecurity standard, but they do offer some interesting viewpoints upon which we can start laying a framework. Further, the use of property-based models is not unheard of in computer cases.[129] In premises liability cases, both the plaintiff and defendant are held to reasonableness standards, starting generally with the requirement that plaintiffs must show that they were injured despite the fact that they were exercising reasonable care for their own safety at the time.[130] Defendant property owners are themselves subject to objective reasonableness tests, generally stemming from the duty of reasonable care owed to all others to prevent injuries that naturally flow from reasonable and foreseeable consequences of their actions.[131]

---

126 *See supra* Section I.B.

127 *See infra* Section II.B.4.

128 *See infra* Part III.

129 *See, e.g.*, Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143 (2016).

130 *See, e.g.*, Fisher v. United States, 705 F. Supp. 2d 57, 72 (D. Mass. 2010) (describing a plaintiff who was obligated to exercise reasonable care for their own safety while inspecting the crawl space of defendant's property); Collins v. East R.S., Inc., 492 S.E.2d 351, 352 (Ga. Ct. App. 1997) (stating a plaintiff must show that they were exercising due care, yet still failed to see the danger); Finazzo v. Fire Equip. Co., 918 N.W.2d 200, 210 (Mich. Ct. App. 2018) ("The reasonableness of defendants' conduct must be weighed against the principles that persons lawfully on the site must use good judgment and common sense for their own safety."); Presbrey v. James, 781 N.W.2d 13, 18 (Minn. Ct. App. 2010) ("The entrant also has a duty to use reasonable care, which may vary based on the circumstances.").

131 *See, e.g.*, Forsythe v. Clark USA, Inc., 864 N.E.2d 227, 238 (2007) ("[I]t is axiomatic that every person owes to all others a duty to exercise ordinary care to guard against injury which naturally flows as a reasonably probable and foreseeable consequence of his act." (quoting Frye v. Medicare–Glaser Corp., 605 N.E.2d 557 (Ill. 1992))); Schur v. L.A. Weight Loss Ctrs., Inc., 577 F.3d 752, 766 (7th Cir. 2009) ("It is well settled that every person owes a duty of ordinary care to all others to

For our purposes, the reasonableness tests of particular interest are those that apply to the duties property owners owe to invitees and licensees.[132] There is some variation in how courts view the distinction of duties owed based on the status of persons on a property owner's premises, but the common law approach is that landowners generally owe a duty of ordinary care to invitees,[133] while they only owe a duty to warn of known concealed dangers and avoid unreasonably dangerous conduct to licensees.[134] It is relevant to this Article why the law has created such a distinction. The most common explanation centers on injuries to

---

guard against injuries which naturally flow as a reasonably probable and foreseeable consequence of an act, and such a duty does not depend upon contract, privity of interest or the proximity of relationship, but extends to remote and unknown persons." (quoting Widlowski v. Durkee Foods, 562 N.E.2d 967, 968 (Ill. 1990))).

132 It is worth noting that contemporary courts applying tort law have removed or significantly eroded the distinctions between invitees, licensees, and even trespassers in some cases. In *Rowland v. Christian*, for example, the California Supreme Court removed the traditional distinctions between parties on or in a property and substituted it with a duty to exercise reasonable care. 443 P.2d 561, 568–69 (Cal. 1968), *superseded by statute*, CAL. CIV. CODE § 847 (West 1985), *as recognized in* Calvillo-Silva v. Home Grocery, 968 P.2d 65, 68–69, 71–72 (Cal. 1998) (observing that Section 847 of California's Civil Code, passed after *Rowland*, limits the liability of an owner of any estate or other interest in real property for injuries that occur upon the property during or after the injured person's commission of any one of twenty-five enumerated felonies).

133 *See, e.g.*, Armstrong v. Ga. Marble Co., 575 So. 2d 1051, 1053 (Ala. 1991) (stating that the owner of the premises owes a duty to business invitees to use reasonable care and diligence to keep the premises in a safe condition, or, if the premises are in a dangerous condition, to give sufficient warning so that, by the use of ordinary care, the danger can be avoided); Riddle v. McLouth Steel Prods. Corp., 485 N.W.2d 676, 679 (Mich. 1992), *reh'g denied*, 488 N.W.2d 736 ("[A] premises owner must maintain [their] property in a reasonably safe condition and has a duty . . . to protect invitees from conditions that might result in injury."); Martin v. City of Washington, 848 S.W.2d 487, 493 (Mo. 1993) (en banc) ("The duty owed by possessors of land to invitees includes the duty to eliminate or warn of dangerous conditions which the defendant knows or in the exercise of reasonable care should have known[;] [i]t [] includes the duty to inspect the premises to discover possible dangerous conditions not known to the occupier."); Van Essen v. McCormick Enters., Co., 599 N.W.2d 716, 719 (Iowa 1999) (providing that the possessor of the premises is under a duty to use ordinary care to keep their premises "in a reasonably safe condition for business invitees"); General Motors Corp. v. Hill, 752 So. 2d 1186, 1187 (Ala. 1999) ("[A landowner is] under a duty to use reasonable care and diligence to keep the premises in a safe condition, or, if the premises [are] in a dangerous condition, to give sufficient warning so that, by use of ordinary care, [an invitee can] avoid the danger." (quoting *Ex parte* Indus. Distrib. Servs. Warehouse, Inc., 709 So. 2d 16, 19 (Ala. 1997))).

134 *See, e.g.*, Heigle v. Miller, 965 S.W.2d 116, 120 (Ark. 1998) (providing that a landowner has a duty to refrain from injuring a licensee through willful or wanton misconduct and to warn a licensee of hidden dangers); Young v. Eriksen Constr. Co., 553 N.W.2d 143, 146 (Neb. 1996) ("An owner or occupant of a premises owes only the duty to refrain from injuring a licensee by willful or wanton negligence or designed injury, or to warn him or her as a licensee of a hidden danger or peril known to the owner or occupant but unknown or unobservable by the licensee, who is required to exercise ordinary care."); Harris County v. Eaton, 561 S.W.2d 245, 247 (Tex. App. 1978), *aff'd*, 573 S.W.2d 177 (Tex. 1978) (outlining a duty by county to warn licensee of danger from chughole).

trespassers, which holds that a property owner should not be required to foresee the presence of those who enter the property unlawfully.[135]

It is worth looking at the elements necessary for a plaintiff to successfully bring a premises liability case. First, the plaintiff must show that the premises' condition presented an unreasonable risk of harm, and may also be required to show that the defendant had actual or constructive knowledge of the condition.[136] Some courts, however, allow a plaintiff to satisfy the knowledge or notice requirement by showing that their injury was attributable to a reasonably unsafe condition related to the property owner's "chosen mode of operation."[137] This latter approach

---

135 The Restatement (Third) of Torts: Liability for Physical and Emotional Harm observes that

> [l]argely for historical reasons, the duty of a land possessor has not been a general duty of reasonable care but, instead has consisted of differing duties depending on the status of the person on land. At the time these status-based duties were developed, no general care of duty existed, and duties were based on relationships or specific activities. Thus, the status-based duties imposed on land possessors were consistent with basic negligence law and were the basis for imposing *any* duty on land possessors.

RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL AND EMOTIONAL HARM ch. 9, § 51 cmt. a (AM. L. INST. 2012). The Restatement, however, rejects status-based duty rules and instead applies a single duty of reasonable care to entrants on land, noting that "with the evolution of a general duty of reasonable care to avoid physical harm . . . , the status-based duties for land possessors are not in harmony with modern tort law." *Id.*

136 *See, e.g.*, Thomas v. E-Z Mart Stores, Inc., 102 P.3d 133, 140 (Okla. 2004) ("An invitor cannot be held responsible unless it can be shown that he/she had notice or could be charged with gaining knowledge of the condition in sufficient time to effect its removal or to give warning of its presence." (quoting Taylor v. Hynson, 856 P.2d 278, 281 (Okla. 1993))); Hawkins v. U.S. Sports Ass'n, Inc., 633 S.E.2d 31, 35 (2006) (stating that an owner must have had actual or constructive knowledge of the defective condition which caused the injury); City of Denton v. Paper, 376 S.W.3d 762, 767 (Tex. 2012) (stating that to prove actual knowledge of the dangerous condition, the plaintiff must show that at the time of the incident, the landowner knew about the dangerous condition).

137 *See, e.g.*, Prioleau v. Kentucky Fried Chicken, Inc., 122 A.3d 328, 335 (N.J. 2015) (discussing how under the mode-of-operation rule, an invitee who is injured is entitled to an inference of negligence and is relieved of the obligation to prove that a business owner had actual or constructive notice of the dangerous condition that caused the accident). The court observed that "[t]he burden imposed on a plaintiff invitee is substantially altered in settings in which the mode-of-operation rule applies. The rule gives rise to a rebuttable inference that the defendant is negligent, and obviates the need for the plaintiff to prove actual or constructive notice." *Id.*

The motivation for such a rule is articulated in *Sarkisian v. Concept Restaurants, Inc.* in the context of a slip-and-fall case:

> Given that the notice inquiry in slip and fall cases is generally a factor of how long the dangerous substance has been on the floor, we concluded that it would be "'unjust to saddle the plaintiff with the burden of isolating the precise failure' that caused an injury, particularly where a plaintiff's injury results from a foreseeable risk of harm stemming from an owner's mode of operation." . . . Accordingly, we held that the notice requirement would be satisfied where "a plaintiff proves that an unsafe condition on an owner's premises exists that was reasonably foreseeable, resulting from an owner's self-

does not, however, obviate the need for a plaintiff to prove notice of an unreasonably unsafe condition, as it is limited to cases where the defendant's chosen mode of operation—for example, serving drinks on a dance floor where spilled liquids could cause invitees to slip—creates unsafe conditions that a reasonable person applying common sense could foresee.

The second element requires the plaintiff to show that the unreasonably unsafe condition was created by the property owner, or that it had existed long enough to allow the owner to know about it and fix it.[138] Note, however, that the duty of the property owner to keep their premises in reasonably safe condition for invitees is not generally delegable. That is, property owners are liable for the negligence of contractors the owner uses for property repairs.[139] This latter aspect may be useful later when considering a software manufacturer's duties to maintain reasonable cybersecurity.[140]

Finally, a premises liability plaintiff must show that the unreasonably unsafe condition was the cause of their injury.[141] This last element is not necessarily directly helpful with respect to reasonableness standards, but is still worth noting for this Article's purposes, as questions regarding causation are often found when considering cybersecurity failures.[142]

---

service business or mode of operation, and the plaintiff slips as a result of the unsafe condition."

Sarkisian v. Concept Rest., Inc., 32 N.E.3d 854, 857–58 (Mass. 2015) (citations omitted) (first quoting Sheehan v. Roche Bros. Supermarkets, Inc., 863. N.E.2d 1276, 1284 (2007); then quoting *id.* at 1286).

138 *See, e.g.*, Ross v. Otis Elevator Co., 539 P.2d 731, 733 (Okla. 1975) ("Where injury to an invitee results from a dangerous condition not created by proprietor but traceable to persons other than those for whom he is responsible, proof that proprietor was negligent with respect to such condition requires a showing that he had actual notice thereof or that the condition had existed for such length of time that in exercise of ordinary care he should have known of it.").

139 *See* Thomas v. E-Z Mart Stores, Inc., 2004 OK 82, ¶ 2–4, 12–13, 22–29, 102 P.3d 133, 135, 137, 140–41 (providing that a store's duty to the invitee with respect to supplying and maintaining floor mats could not be delegated to the supplier of the floor mats).

140 *See infra* Section III.A.

141 *See* Shaner v. Tucson Airport Auth., Inc., 573 P.2d 518, 521–22 (Ariz. Ct. App. 1977) (denying recovery where there is no causal connection between inadequate lighting and security in lot and abduction); Fender v. Colonial Stores, Inc., 225 S.E.2d 691, 695–97 (Ga. Ct. App. 1976) (providing that there is no liability where the defect is not discoverable by inspection); Letson v. Lowmaster, 341 N.E.2d 785, 787–88 (Ind. Ct. App. 1976) (providing no recovery against campground owner where no evidence alleged negligence was the proximate cause of an eye injury); Manganello v. Permastone, Inc., 231 S.E.2d 678, 680–82 (N.C. 1977) (determining failure to control boisterous play of swimmers is a question for a jury). An absent possessor of land can be charged with constructive notice of a dangerous condition, if they were acting so as to keep themselves ignorant. Warren v. Stancliff, 251 A.2d 74, 76 (Conn. 1968).

142 *See infra* Section III.A.

There are three significant issues for later consideration that arise if we compare circumstances that occur in premises liability cases and those found in cybersecurity failure cases. First, except in specific cases, such as those involving cyber-physical systems, cybersecurity failures will generally not result in physical injury, unlike many of the premises liability cases cited.[143] Second, it is not clear whether and how physical property concepts like entering and trespassing translate to cybersecurity contexts, where devices may be physical, but many of the activities in question are less easily characterized. Third, it is not necessarily straightforward how reasonableness standards regarding, for example, the obviousness of dangers, translate to the complexities of hardware and software.

B. *Deriving Reasonable Cybersecurity from Common Law*

Common law reasonableness, perhaps most often encountered in questions of negligence, is meant to hold liable conduct that puts others at risk of an unreasonable risk of harm, requiring that parties act in ways that are considered reasonable under the circumstances. This reasonableness standard can be defined by a court or legislature, and it is this flexibility, as opposed to the rigidity of a bright-line rule, that makes common law reasonableness particularly useful for determining what are reasonable actions in a data security context. This Section will select aspects of this standard that can help form a basis for a cybersecurity reasonableness framework.

1. Reasonable Cybersecurity and the Duty of Ordinary Care

A particularly interesting example of the application of tort principles of reasonableness to the technology domain can be found in recent state efforts to pass data privacy laws, such as the California Consumer Privacy Act (CCPA).[144] Although not itself strictly a cybersecurity statute, it does take into account the implicit cybersecurity failures that often lead to data breach and privacy issues.[145] Ohio has also passed its own data security law, which also maintains a safe harbor

143 *See* Choi, *supra* note 14, at 42–43.

144 CAL. CIV. CODE § 1798.150(a) (West 2024).

145 CCPA liability may attach if personal data is disclosed "as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information . . . ." CAL. CIV. CODE § 1798.150(a)(1) (2024). Note that this language contains similar situational provisions as the "best available technology" Environmental Protection Agency rules. *See infra* Section II.E.

provision for those who show compliance with certain data protection frameworks.[146] The frameworks enumerated in the Ohio legislation are the National Institute of Standards and Technology (NIST) Cybersecurity Framework and related publications, the Federal Risk and Authorization Management Program (FedRAMP) security assessment framework, the Center for Internet Security Critical Security Controls for Effective Cyber Defense, and other frameworks that apply to specific industries.[147]

These efforts demonstrate a clear move among state officials and legislators toward a cybersecurity reasonableness standard that meets the needs and risks formed by contemporary technology innovations and uses. The legal and political challenges that accompany attempts to create or modify regulations around a growing technology (with an increasingly powerful industry behind it) become especially acute at the federal level, where these complications are magnified by national political fights, agency "turf wars," and the general vagaries of federalism. The recent emergence and growth of state-level data security regulatory efforts indicate that it is not a lack of motivation or justification that prevents similar efforts at the federal level.[148]

As described earlier in this Article, the concept of reasonableness as a standard is attractive both for its demonstrated aspirations toward objectivity as well the flexibility necessary to account for changing norms.[149] Two particularly interesting areas from which a reasonable cybersecurity standard can emerge are in the use of industry customs and practices, especially in products liability cases, and the element of foreseeable harms as it pertains to a standard of ordinary care.

2. Reasonable Cybersecurity and Industry Custom

The use of industry customs and practices as a basis for reasonable cybersecurity can be considered, for our purposes, in two contexts. First, courts may look to the norms of a particular industry when considering negligence cases. Note, however, that the norms associated with particular segments of the technology industry should not be considered to be the same thing as industry cybersecurity guidelines, frameworks, and best practices.[150]

---

146 OHIO REV. CODE ANN. §§ 1354.01–1354.05 (West 2019).

147 *Id.* § 1354.03.

148 *See generally* Scott J. Shackelford, Anne Boustead & Christos Makridis, *Defining "Reasonable" Cybersecurity: Lessons from the States*, 25 YALE J.L. & TECH. 86 (2023).

149 *See supra* Part I.

150 *See infra* Part III.

What should be considered reasonable cybersecurity should consider the relevant characteristics and context related to the specific manufacturer. The flexibility of reasonableness as a standard is crucial here, as the standard as applied to, say, a music-playing application, should not be the same as that of the highly complex set of software systems that make up self or assisted driving vehicles. The standard of care required for scenarios as different in scope, risk, and levels of harm as these should account for these differences appropriately. This is not to say that core software security standards, as defined in the NIST Framework or similar guidelines, should not apply to manufacturers across the board. But any reasonable cybersecurity standard should account for both foreseeability as well as the magnitude of injuries of the case.[151]

But just because a software-driven device does not pose an immediate risk of physical harm, that does not mean that it is necessarily harmless. Internet of Things (IoT) devices occupy a strange zone of risk in the cybersecurity context. These devices are often designed to be both inexpensive and innocuous to the point of being invisible to the consumer, and often forgotten as a source of cybersecurity risk.[152] But the actual risks associated with these innumerable devices are significant and are often best seen in the aggregate. For example, in 2016, hundreds of thousands of IoT devices were hijacked by hackers using malware dubbed "Mirai" to become part of a massive botnet and used to attack a range of targets.[153] Hackers used this botnet to attack OVH, a French telecommunications company, along with many hundreds of thousands of other critical devices, websites, and services around the world.[154] Despite the fact that the vulnerabilities leveraged were on small, cheap devices, the harms that resulted from this cybersecurity failure were quite large.[155] Because of what may appear to be confusing or misleading levels

---

151 *See generally* CYBER-PHYSICAL SYSTEMS: A REFERENCE (Xue Wang ed., 2020).

152 *See, e.g.*, Leta E. Gorman, *The Era of the Internet of Things: Can Product Liability Laws Keep Up?*, DEF. COUNS. J., Jan. 27, 2020, at 3; Mauricio Paez & Mike La Marca, *The Internet of Things: Emerging Legal Issues for Businesses*, 43 N. KY. L. REV. 29, 32–33 (2016) ("Experts predict that [through IoT devices] the Internet will become 'so effortlessly interwoven into daily life that it will become invisible, flowing like electricity.'" (quoting JANNA ANDERSON & LEE RAINE, PEW RSCH. CTR., DIGITAL LIFE IN 2025 5 (2014))).

153 *What Is the Mirai Botnet?*, MALWAREBYTES, https://www.malwarebytes.com/what-was-the-mirai-botnet [https://perma.cc/8F6X-YKEC].

154 *See* Elie Bursztein, *Inside the Infamous Mirai IoT Botnet: A Retrospective Analysis*, CLOUDFLARE (Dec. 14, 2017), https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis [https://perma.cc/6SMP-4ZWN].

155 *See* Press Release, U.S. Atty's Off., Dist. of N.J., Justice Department Announces Charges and Guilty Pleas in Three Computer Crime Cases Involving Significant Cyber Attacks (Dec. 13, 2017), https://www.justice.gov/usao-nj/pr/justice-department-announces-charges-and-guilty-pleas-three-computer-crime-cases [https://perma.cc/8Q7G-GP5R].

of potential harm to courts or jurors, expert testimony will likely prove necessary to properly calibrate levels of reasonable care for software manufacturers.[156]

What makes for constructive industry customs and practices will also depend on how the guidance around those customs is framed. For example, some state and private efforts to set reasonable cybersecurity standards concentrate on the addition of security features at the expense of recommendations for removing insecure features.[157] For example, California's Senate Bill 327 contains provisions that require the addition of security features such as firewalls or antivirus software. There can be two problems with taking this approach.[158] First, adding components to already complex software-based platforms will automatically increase the device's overall complexity, creating more possibilities for cybersecurity vulnerabilities. Second, adding security features in this manner is not generally the best way to actually increase security. It is far better to remove sources of insecurity, such as hardcoded passwords or poor update management.[159] However, a flexible concept of reasonableness should be able to account for these problems.

3. Foreseeable Risk of Injury

Foreseeability is a critical part of any analysis of reasonable conduct or standards of care.[160] In the products liability context, for example, what

---

156 *See, e.g.*, Lucas M. Amodio, *The Intersection of Product Liability Law and the Internet of Things*, 2021 B.C. INTELL. PROP. & TECH. F. 1, 24 (2021) ("Thus far, the courts have held that having a potential for harm due to hacking is not enough, and therefore, the scope of product liability law will not be fully realized until someone is actually physically harmed by a compromised IoT device. Until then it would be advisable for manufacturers of IoT devices to conform their product development to exercise a reasonable standard of care for cybersecurity, such as that proposed by the FTC."). Note also that California Senate Bill 327 requires that, as of January 2020,

> [a] manufacturer of a connected device, as those terms are defined, shall equip the device with a reasonable security feature or features that are all of the following: (1) [a]ppropriate to the nature and function of the device[;] (2) [a]ppropriate to the information it may collect, contain, or transmit[;] [and] (3) [d]esigned to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

S.B. 327, ch. 886, 2017–2018 Leg., Reg. Sess. (Cal. 2018).

157 *See* Robert Graham, *California's Bad IoT Law*, ERRATA SEC. (Sep. 10, 2018), https://blog.erratasec.com/2018/09/californias-bad-iot-law.html#.W6PwnZNKjX8 [https://perma.cc/3L44-Y74D].

158 *Id.*

159 *Id.*

160 *See* Kristine Cordier Karnezis, Annotation, *Products Liability: Modern Cases Determining Whether Product Is Defectively Designed*, 96 A.L.R.3d 22 (1979).

a court considers reasonable care must take into account what was reasonably foreseeable at the time the product's design was put into use.[161] More to the point, a question of reasonableness will depend on whether the manufacturer could have foreseen that their design could potentially be harmful.[162] But as is the case with establishing reasonable alternative designs, manufacturers will argue that most software failures, particularly the exploitation of security vulnerabilities, were unanticipated by their designers, creating an explosion of questions, some of them unanswerable, to be considered by courts.[163]

Because of software's complex nature, as well as the potential complexity of the software development process, we will always be able to find vulnerabilities in software-based products. This does not mean, however, that none of these vulnerabilities could have been anticipated by software developers at the time of design. Memory safety vulnerabilities, for example, have long been the source of successful hacks on software, accounting for seventy percent or more of reported software security vulnerabilities.[164] Many of these vulnerabilities can be attributed to design or programmer error, where lack of experience and knowledge of these issues can play a large role. Because of this, numerous pointers, guides, and best practices documents identify memory safety issues as a serious problem and provide information on avoiding them.[165] Nevertheless, memory safety issues continue to be a serious source of cybersecurity failures.[166] Surely, under circumstances like these, where industry best practices clearly illustrate a particular danger in software design, manufacturers should find it more difficult to argue that such vulnerabilities were unforeseeable.

---

161 *Id.*

162 *See, e.g.*, Bandstra v. Int'l Harvester Co., 367 N.W.2d 282, 286 (Iowa Ct. App. 1985). Section 2(b) of the Restatement (Third) of Torts: Products Liability states that

> [a] product . . . is 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 by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the alternative design renders the product not reasonably safe.

RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2(b) (AM. L. INST. 1998).

163 *See supra* Section II.A.

164 *See* Paul C. van Oorschot, *Memory Errors and Memory Safety: C as a Case Study*, 21 IEEE SEC. & PRIV. 70, 70 (2023).

165 *See, e.g.*, NAT'L SEC. AGENCY, SOFTWARE MEMORY SAFETY (2023).

166 *See, e.g.*, Bob Lord, *The Urgent Need for Memory Safety in Software Products, Cybersecurity & Infrastructure Security Agency*, CISA (Dec. 6, 2023), https://www.cisa.gov/news-events/news/urgent-need-memory-safety-software-products [https://perma.cc/8N5E-R92J].

4. Reasonable Alternative Design

As we increase our dependence on software-based technologies, especially—but not exclusively—those that can cause physical injury when they fail, the idea of liability for software manufacturers whose product designs are flawed or vulnerable to failure is an attractive one. There has been considerable difficulty, however, in finding an acceptable application of design defect jurisprudence to software.[167] That is, when one looks at the software development process, it can be tricky to cleanly delineate between its design and manufacturing stages. Significant disagreement among experts regarding optimal software designs and algorithm choices makes this analysis complicated and expensive, often leading to confusion and frustration for courts which often turn to modifications of existing standards.[168]

The difficulties in establishing a basis for cybersecurity reasonableness are numerous and significant. If, for example, we adopt an approach that assumes that any unanticipated outcome by the software manufacturer is, by definition, a defect in their design, then any failure could have been reasonably avoided if the design had properly accounted for it. But all software failures are, to varying degrees, unanticipated (assuming no manufacturer malice), so the challenge then becomes one of separating which of these failures should have been reasonably foreseen during the software design process.[169] However, given the inherent complexity of the software development process and

---

167 *See* 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, 915 (2017).

168 *See, e.g.*, Mark A. Geistfeld, *A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation*, 105 CALIF. L. REV. 1611, 1642–46 (2017) (describing the "modified consumer expectations test" (quoting Izzarelli v. R.J. Reynolds Tobacco Co., 136 A.3d 1232, 1242 (Conn. 2016) ("Under the 'modified' consumer expectations test, the jury would weigh the product's risks and utility and then inquire, in light of those factors, whether a reasonable consumer would consider the product design unreasonably dangerous.")")).

169 *See, e.g.*, Gary E. Marchant & Rachel A. Lindor, *The Coming Collision Between Autonomous Vehicles and the Liability System*, 52 SANTA CLARA L. REV. 1321, 1334 (2012) ("The problem is that most accidents will result from situations that the manufacturer or designer did not anticipate. This will open the manufacturer to second-guessing by the plaintiff's expert that an adjustment would have provided a safer alternative system that would have avoided the accident in question. The manufacturer will almost always lose the cost-benefit argument, conducted in hindsight in the litigation context, when it focuses at the micro-scale between slightly different versions of the autonomous system. This is because the cost of not implementing the potential improvement will usually be severe—the loss of one or more lives or other serious injury, compared to the relatively small cost of the marginal improvement that might have prevented the accident." (footnote omitted)).

the resulting software products themselves, these questions will quickly become frustrating to parties as well as courts.[170]

This is where applicable regulations and established cybersecurity guidelines become important to reasonable cybersecurity design. As federal and state regulators establish their authority in this domain, rules that take into account consumer harms due to cybersecurity failures, especially when considered in an aggregated sense, can form a set of baselines upon which reasonableness analyses may credibly rest.[171] For example, a regulatory framework that contains some analog to best available technology standards as they have been applied in clean air and water contexts could serve as guidelines for reasonable alternative design arguments.[172] Similarly, cybersecurity best practices and related industry guidelines also create strong starting points for asserting reasonable alternative designs based on these established industry norms.[173]

5. Negligence Per Se

In cases involving companies that have experienced data breaches, courts have become more willing to consider claims against them for negligence per se. A negligence per se claim "is established by showing a statute created a duty to the plaintiff and the defendant breached that duty by violating the statute;" the plaintiff may also be required to show that they are "within the class of persons intended to be protected by the statute and that the statute was meant to protect against the harm suffered."[174] These claims have become more likely to gain traction as federal authorities—especially the FTC—have established their own rigorous standards for what should be considered reasonable cybersecurity practices.[175] It should be noted, however, that "negligence per se is 'not liability per se,'" such that even if negligence per se can be

---

170 *See, e.g.*, Kenneth S. Abraham & Robert L. Rabin, *Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era*, 105 VA. L. REV. 127, 143–44 (2019).

171 *See, e.g.*, Derek Bambauer, *Cybersecurity for Idiots*, 106 MINN. L. REV. HEADNOTES 172, 182 (2021).

172 *See infra* Section II.E.

173 *See infra* Section II.D.

174 *See* Seals by Causey v. Winburn, 445 S.E.2d 94, 96 (S.C. Ct. App. 1994); *In re* Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1327 (N.D. Ga. 2019); Whitlaw v. Kroger Co., 410 S.E.2d 251, 252 (S.C. 1991) ("In order to show that the defendant owes him a duty of care arising from a statute, the plaintiff must show two things: (1) that the essential purpose of the statute is to protect from the kind of harm the plaintiff has suffered; and (2) that he is a member of the class of persons the statute is intended to protect."(quoting Rayfield v. S.C. Dep't of Corr., 374 S.E.2d 910, 914 (S.C. Ct. App. 1988))).

175 *See infra* Section II.C.

shown, plaintiffs must still prove proximate causation and actual damages to recover.[176]

In *In re Blackbaud, Inc.*, a federal district court considered a class action against a data collection and storage company for injuries resulting from a data breach.[177] Among the plaintiffs' claims was an action for negligence per se based on Blackbaud's alleged violations of the FTC Act, the Healthcare Insurance Portability and Accountability Act (HIPAA), and the Children's Online Privacy Protection Act (COPPA).[178] The court observed that states are split on the question of the FTC Act as a potential basis for negligence per se claims regarding data breaches, pointing to the different standards for negligence per se in the various jurisdictions.[179] The plaintiffs in *Blackbaud* failed to state this claim, in the court's opinion, as they did not sufficiently show that they were members of the class the FTC Act was meant to protect, which was likely more a problem with the wording of the plaintiffs' pleadings than with the broad applicability of the FTC Act.[180] Despite the failure of the *Blackbaud* plaintiffs, however, it is likely that we will see more successful claims of negligence per se going forward, mainly due to the work the FTC has done to help define cybersecurity reasonableness.

C. *Regulatory Reasonableness*

As data security incidents rose alongside the increasingly rapid proliferation of computers and networks in the late 1990s and 2000s, questions about legal means of recourse and prevention revealed something of a regulatory gap. The FTC stepped in to fill this through its authority over unfair and deceptive trade practices, broadening enforcement to require companies to take "reasonable" or "appropriate" security precautions.[181] As the FTC undertook investigations of consumer

176 *Equifax*, 362 F. Supp. 3d at 1328 (citations omitted).

177 *In re* Blackbaud Inc., Customer Data Breach Litig., 567 F. Supp. 3d 667, 672 (D.S.C. 2021).

178 *Id.* at 683.

179 *Id.* at 684.

180 *Id.* at 684–85.

181 *See* Protecting Our Nation's Cyberspace: Hearing Before the H. Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, 108th Cong. 2–6 (2004) (statement of Orson Swindle, Comm'r,, FTC), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-protecting-our-nations-cyberspace/042104cybersecuritytestimony.pdf [https://perma.cc/WHT8-Y3UM] (articulating the Commission's role in protecting information security, highlighting the essential functions computers play in our everyday lives, and acknowledging that while "breaches can occur even when a company has taken all reasonable precautions[,]" failures to take cybersecurity measures that are "appropriate under the circumstances" become risks to consumer data).

cybersecurity incidents, they often reached consent decrees with the companies found to have failed to take these reasonable or appropriate steps to protect their customers' data.[182] To fully address a growing list of data security cases, the FTC created the Division of Privacy and Identity Protection within its Bureau of Consumer Protection to "oversee[] issues related to consumer privacy, credit reporting, identity theft, and information security."[183] This division has grown to take on a wide array of technology and data-related cases, to include such recent areas as artificial intelligence, health privacy, children's privacy, and geolocation data complaints, bringing eighty-nine data security cases since 1999.[184] This large collection of consent orders has built, in the words of Dan Solove and Woodrow Hartzog, a "common law" of jurisprudence and principles from which one can extrapolate rules of reasonable cybersecurity practices.[185]

The *Wyndham* and *LabMD* cases, introduced in Part I, were something of watershed cases for the FTC, as they both confirmed the FTC's authority to oversee data security practices but also placed new requirements on the specifics the agency must provide in its complaints and consent orders, further refining and adding detail to the set of reasonable cybersecurity rules.[186] Both the *Wyndham* and *LabMD* courts considered two core questions: whether the FTC has the authority to regulate cybersecurity under the unfairness prong of Section 5 of the FTC Act, and whether the companies had fair notice as to their specific cybersecurity practices falling outside of that unfairness provision.[187] The *Wyndham* court agreed that the hotel company's cybersecurity practices fell within the plain meaning of "unfair," comparing it to analogous scenarios in the physical world where potentially hundreds of thousands of customers could be injured.[188] Further, the court rejected Wyndham's argument that the FTC complaint was too vague to implement,

---

182 *See, e.g.*, *In re* TJX Cos., Inc., A Corp., No. 72-3055, 2008 WL 903808, at *5 (F.T.C. Mar. 27, 2008) (ordering TJX, inter alia, to "provide reasonable assurance that the security, confidentiality, and integrity of personal information [on company networks] is protected" following an investigation into a data breach).

183 *Division of Privacy and Identity Protection*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity [https://perma.cc/J2CP-9233].

184 Press Release, Fed. Trade Comm'n, FTC Releases 2023 Privacy and Data Security Update (Mar. 28, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/03/ftc-releases-2023-privacy-data-security-update [https://perma.cc/M7ES-3CAS].

185 Solove & Hartzog, *supra* note 8, at 585–86.

186 Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d, 236, 249, 258 (3rd Cir. 2015); LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1235–36 (11th Cir. 2018); *see supra* Part I.

187 *Wyndham*, 799 F.3d at 240; *LabMD*, 894 F.3d at 1224.

188 *Wyndham*, 799 F.3d at 247.

concluding that it was sufficient to put the company on notice of possible liability under the FTC Act.[189] The *LabMD* court, on the other hand, ended up ruling against the FTC, assuming for the sake of argument that the FTC had some authority to regulate cybersecurity, but holding that the FTC's complaint alleged no specific unfair acts or practices.[190] The court saw the installation of the software that led to the data breach as a singular event, rejecting the FTC's more holistic view of the company's cybersecurity practices.[191] These cases, especially *LabMD*, caused the FTC to tighten up its data security enforcement practices, making its cybersecurity orders more specific, all of which made the FTC requirement of "reasonableness" in data security standards more robust as a widely adopted standard.[192]

D. *Technology-Based Standards of Reasonableness*

The fact that ensuring cybersecurity is a hard problem is well-established.[193] There is an old saying among information security professionals that says: those who seek to protect a system's security need to be right every time; those who seek to break a system's security need only be right once. The technological systems we continue to use and rely upon daily are already quite complicated and the interconnectedness of these stems only worsens the complexity.[194] If complexity is the enemy of security, then conventional wisdom would hold that we are doomed to keep digging ourselves ever deeper into a cybersecurity hole.

---

189 *Id.* at 258.

190 *Id.*

191 *LabMD*, 894 F.3d at 1237.

192 *See* Press Release, Fed. Trade Comm'n, FTC Announces Sessions on Consumer Privacy and Data Security as Part of Its Hearings on Competition and Consumer Protection in the 21st Century (Oct. 26, 2018), https://www.ftc.gov/news-events/news/press-releases/2018/10/ftc-announces-sessions-consumer-privacy-data-security-part-its-hearings-competition-consumer [https://perma.cc/UFS2-V7UZ].

193 *See generally* Robert Ghanea-Hercock, *Why Cyber Security Is Hard*, 2012 GEO. J. INT'L AFFS. 81; Natalie M. Scala, Allison C. Reilly, Paul L. Goethals & Michel Cukier, *Risk and the Five Hard Problems of Cybersecurity*, 39 RISK ANALYSIS 2119 (2019); Michael Daniel, *Why Is Cybersecurity So Hard?*, HARV. BUS. REV. (May 22, 2017), https://hbr.org/2017/05/why-is-cybersecurity-so-hard [https://perma.cc/CJR6-3DLQ]; Elena Kvochko, *Why Cyber Security Is Still* So *Complex*, FORBES (Oct. 25, 2020), https://www.forbes.com/sites/elenakvochko/2020/10/25/why-cyber-security-is-still-so-complex [https://perma.cc/KF65-Y2RC].

194 *See* Eric Jardine, *Taking the Growth of the Internet Seriously When Measuring Cybersecurity*, *in* RESEARCHING INTERNET GOVERNANCE: METHODS, FRAMEWORKS, FUTURES 145 (Laura DeNardis, Derrick L. Cogburn, Nanette S. Levinson & Francesca Musiani eds., 2020); Gary McGraw, *Software Security*, 2 IEEE SEC. & PRIV. 80 (2004).

While this is all true as far as it goes, a large, sophisticated industry of information security professionals has been actively working to mitigate cybersecurity risks.[195] This industry has grown out of an early awareness of the problems that would inevitably arise as we grew more dependent upon computers and networks, and has been working along multiple axes to address cybersecurity failures as and after they occur.[196] But, even more importantly, the industry tries to prevent these failures from happening in the first place through the careful development of cybersecurity best practices.[197] This field has relevance across multiple disciplines and use cases, so some of the issues raised and addressed are specific to certain contexts.[198] But there are core principles that have emerged over the past few decades that remain applicable across technology domains.

1. The NIST Framework

Perhaps the most widely known collection of these principles is found in the NIST Cybersecurity Framework.[199] NIST, part of the U.S. Department of Commerce, started putting together a collection of cybersecurity best practices in 2013 based on the accumulated work and wisdom from multiple sources since the 1980s.[200] U.S. presidents since that time have generally taken an incrementalist approach to cybersecurity with little to no legislative or regulatory efforts behind them. In 2009, President Obama identified security vulnerabilities to the nation's critical digital infrastructure, which he declared as a "strategic national asset."[201] Seeing little interest from Congress to create legislation to protect this asset, President Obama issued an executive order in 2013 that established the NIST Framework as a collection of cybersecurity best

---

195 *See, e.g.*, Amanda N. Craig, Scott J. Shackelford & Janine S. Hiller, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52 AM. BUS. L.J. 721 (2015).

196 The literature in this area is both copious and constantly changing, for obvious reasons. *See, e.g.*, WILLIAM STALLINGS, EFFECTIVE CYBERSECURITY: A GUIDE TO USING BEST PRACTICES AND STANDARDS (2018).

197 *Id.*

198 *See* Exec. Order No. 13,636, 78 Fed. Reg. 11737 (Feb. 12, 2013).

199 NAT'L INST. STANDARDS & TECH., THE NIST CYBERSECURITY FRAMEWORK (CSF) 2.0 (2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf [https://perma.cc/4UU6-2FVE].

200 If one were to mark the moment at which the U.S. federal government first took serious notice of cybersecurity issues, it might be when the Morris Worm was released on an early internet in 1988. *See* Scott Shackelford, *Another 'Back to the Future' Moment—27 Years After the World's First Cyber Attack*, HUFFPOST (Oct. 30, 2015), https://www.huffpost.com/entry/another-back-to-the-future-moment_b_8428352 [https://perma.cc/D2GD-66G8].

201 Barack Obama, Pres., Remarks on Securing the Nation's Information and Communications Infrastructure (May 29, 2009), *in* 2009 DAILY COMP. PRESS DOC. 410 .

practices to be applied by manufacturers and implementors of computer technologies.[202]

From its beginning, the NIST Framework was not meant to be a federal policy imposed upon industries out of some office in Maryland, but was rather a product of multiple meetings involving representatives from multiple nations across multiple industries.[203] Each such meeting built upon the goals and outcomes of the previous meetings, with Version 1.0 of the Framework finally becoming published on February 12, 2014.[204] Since that time, subsequent updates have arisen out of continued workshops as well as new legislation, culminating in the current—but not final—version of the Framework.[205] As of this writing, NIST is currently collecting additional comments and information in their effort to compile and release Version 2.0 of the Framework.[206]

A full description of the NIST Cybersecurity Framework is beyond the scope of this Article due in large part to the Framework's sheer breadth. Rather, a summary of the Framework's acceptance and use is more applicable to an analysis of its place in building a notion of reasonable cybersecurity.[207] The practices articulated within the Framework, created through a collaborative process involving hundreds across multiple industries and interests, reflect accepted wisdom by experts and professionals through guidelines meant to address the largest percentage of the most critical problems as practicable. The Framework thus establishes a baseline rather than a ceiling for cybersecurity best practices—what we should consider as reasonable behavior by technology manufacturers.[208]

Use of the NIST Cybersecurity Framework as a measure for reasonableness is gaining traction among regulators. The Department of Justice guidelines recommend that companies apply the Framework, referred to as a reference standard for cybersecurity by information

---

202 Exec. Order No. 13,636, *supra* note 198.

203 *History and Creation of the CSF 1.1*, NAT'L INST. STANDARDS & TECH., https://www.nist.gov/cyberframework/ history-and-creation-framework [https://perma.cc/V94R-AMWT].

204 *Id.*

205 *See Framework Development Archive*, NAT'L INST. OF STANDARDS & TECH., https://www.nist.gov/cyberframework/framework/framework-development-archive [https://perma.cc/6TQK-QXDF]; Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 (2014).

206 *NIST's Journey to CSF 2.0*, NAT'L INST. OF STANDARDS & TECH., https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20 [https://perma.cc/FU8C-86BJ].

207 For a more detailed analysis of the NIST Framework itself, see Scott J. Shackelford, Scott Russell & Jeffrey Haut, *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, 16 U.C. DAVIS BUS. L.J. 217, 219–20 (2016).

208 *Id.*

security consultants.[209] The recommended use of the Framework is not limited to federal guidance. For example, the Ohio Data Protection Act contains a safe harbor provision against state tort actions for cybersecurity failures within businesses that implement a cybersecurity program based on the Framework.[210] And, perhaps most importantly, the standard legal advice for companies manufacturing, selling, and implementing computer technologies is to build a functioning cybersecurity system around the NIST Framework.[211]

The NIST Framework is a sprawling set of documents, so it may be best to start by focusing on a particular publication, *Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53* ("800-53").[212] This document is widely supported across the technology industry, and the fact that other international standards and policies significantly overlap or rely on 800-53, gives strong evidence of the standard's usefulness as source of cybersecurity reasonableness.[213] For example, of seventy-two "reasonable practices" collected from FTC complaints and consent decrees, sixty-six of them were directly or indirectly covered by 800-53.[214] These widely known and accepted best practices can surely guide reasonable cybersecurity choices.

---

209 Sheila A. Millar, Tracy P. Marshall & Nathan A. Cardon, *Takeaways from NIST's Updated Cybersecurity Framework*, LAW360 (Feb. 6, 2017, 1:20 PM), https://www.law360.com/articles/888535/takeaways-from-nist-s-updated-cybersecurity-framework [https://perma.cc/NP5N-QJZ5].

210 *See* OHIO REV. CODE ANN. §§ 1354.02–1354.03 (West 2018).

211 *See, e.g.*, Dean Forbes & Shay Banerjee, *Enterprise-Level Targeted Guidance: An Approach to Cybersecurity Risk Oversight for Corporate Directors*, IN-HOUSE DEF. Q., Spring 2018; *Why You Should Adopt the NIST Cybersecurity Framework*, PRICE WATERHOUSE COOPERS (May 2014), http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf [https://perma.cc/5JM8-RYQH] ("[T]he Framework comprises leading practices from various standards bodies that have proved to be successful when implemented, and it also may deliver regulatory and legal advantages that extend well beyond improved cybersecurity for organizations that adopt it early.").

212 NAT'L INST. OF STANDARDS & TECH., SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS 800-53 (2013).

213 *See* Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703, 745 (2016).

214 Kristina Rozan, *How Do Industry Standards for Data Security Match Up with the FTC's Implied "Reasonable" Standards—And What Might This Mean for Liability Avoidance?*, INT'L ASS'N PRIV. PROS. (Nov. 25, 2014), https://privacyassociation.org/news/a/how-do-industry-standards-for-data-security-match-up-with-the-ftcs-implied-reasonable-standards-and-what-might-this-mean-for-liability-avoidance [https://perma.cc/GP7Y-EHNV].

2. Government and Private Cybersecurity Advisories

The cybersecurity experiences of the past few decades have put governments around the world on notice, illustrating the necessity of developing coherent cybersecurity strategies in order to protect critical infrastructure, punish and deter cybercrime, encourage economic growth, and protect their citizens' civil rights online.[215] Because networks and computing technologies' emergence and adoption is highly dynamic, they become increasingly difficult to manage and protect, especially as the techniques of attackers become increasingly sophisticated and complex.[216] The U.S. government has gone through a number of cycles and attempts at governing and protecting American networks and systems (both public and private), from early ideas about critical infrastructure protection by the second Clinton administration, to more rigorous efforts, culminating in the creation of the Cybersecurity and Infrastructure Security Agency (CISA) under the Department of Homeland Security.[217]

CISA takes much of its mandate from the 2013 Presidential Policy Directive 21, which defined sixteen critical infrastructure sectors whose destruction or compromise would have severe or catastrophic effects on the country.[218] In order to facilitate the protection of these sectors, CISA, along with government and industry partners, monitors current threat models and attack intelligence, compiling its findings into databases for trend and pattern analysis, and publishing its findings through reports and alerts.[219] These publications can range from general advice and best practices to real time advisories and alerts regarding current and emerging cyber threats and vulnerabilities, but taken collectively, they

---

215 *See* ORG. ECON. COOP. & DEV., CYBERSECURITY POLICY MAKING AT A TURNING POINT: ANALYZING A NEW GENERATION OF NATIONAL CYBERSECURITY STRATEGIES, DSTI/ICCP/REG(2011)12/FINAL (Nov. 16, 2012).

216 *See, e.g.*, Atif Ahmad, Jeb Webb, Kevin C. Desouza & James Boorman, *Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack*, 86 COMPUTS. & SEC. 402, 402–03 (2019); Pooneh Nikkhah Bahrami et al., *Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures*, 15 J. INFO. PROCESSING SYS. 865, 865 (2019); Julian Jang-Jaccard & Surya Nepal, *A Survey of Emerging Threats in Cybersecurity*, 80 J. COMPUT. & SYS. SCIS. 973, 973–74 (2014).

217 *See* ANDY GREENBERG, SANDWORM: A NEW ERA OF CYBERWAR AND THE HUNT FOR THE KREMLIN'S MOST DANGEROUS HACKERS (2019); *About CISA*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/about [https://perma.cc/G483-YNCB].

218 Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience, 2013 PUB. PAPERS 106 (Feb. 12, 2013).

219 *Cyber Threats and Advisories*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/cyber-threats-and-advisories [https://perma.cc/22TJ-MPJR].

can provide a comprehensive basis for what can be considered reasonable cybersecurity.

What is particularly useful about these various CISA publications is the fact that they are not only organized by attacker activities and platform vulnerabilities, but can be interpreted and filtered to account for the kinds of case-by-case scenarios that will occur across industries and technology use cases.[220] For example, the CISA alerts, published in coordination with the National Cyber Awareness System, organize its advisories around specific threat group activities, use of malware or other software hacking tools, vulnerabilities in hardware and software platforms, and actionable recommendations for securing technologies from the threat.[221] Collectively, these alerts and advisories can create a foundation upon which reasonable cybersecurity behavior can be derived; what Cass Sunstein has called "regulation through disclosure."[222]

Alongside these CISA publications, and often in coordination with CISA and other government agencies, private cybersecurity firms also provide their own framework of advisories and alerts that can further augment a reasonableness background. Falling under the umbrella term of "cyber threat intelligence" ("CTI"), these publications are offered as a means to avoid the data overload that can come with the territory and are organized into threat intelligence platforms to aggregate and organize the cybersecurity threat information by category.[223] The point of these CTI platforms is to take the raw data regarding security threats, vulnerabilities, exploits, and malware, and organize and present that information in a way that can directly provide support for cybersecurity-related decisions—just the sort of widely available and easily accessible information that could be considered as a basis for reasonable cybersecurity actions.

E. *A Two-Way Conversation with Regulatory Law and Industry*

---

220 *Resources & Tools*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/resources-tools [https://perma.cc/X6JT-EGC8]; *CISA Gateway*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/resources-tools/services/cisa-gateway [https://perma.cc/JC72-3PCR].

221 *Cybersecurity Alerts & Advisories*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/news-events/cybersecurity-advisories [https://perma.cc/H8H3-G6LE].

222 Cass R. Sunstein, *Informational Regulation and Informational Standing: Akins and Beyond*, 147 U. PA. L. REV. 613, 613 (1999).

223 Cyber Threat Intelligence Platforms are offered by such providers. *See* IBM X-FORCE, https://exchange.xforce.ibmcloud.com [https://perma.cc/R9DB-4SY2]; *Threat Intelligence: Driving the Future of Security*, CHECKPOINT, https://www.checkpoint.com/solutions/threat-intelligence-research [https://perma.cc/E5EP-M4PJ]; *Threat Intelligence & Hunting*, CROWDSTRIKE, https://www.crowdstrike.com/products/threat-intelligence [https://perma.cc/A7DJ-7TS6].

Standards

Beyond the realm of regulatory law, reasonableness, especially in the context of tort law, is especially important to the bigger picture goal of law that goes beyond the mere settlement of accounts between aggrieved private actors. Rather, the use of the reasonableness standard can be seen as a foundational element of socially desirable policy outcomes. This framing sees torts not (only) as private law but as public law, a collective means of spreading losses and establishing accountability—especially for manufacturers of consumer products—that might otherwise fall between the cracks of overtaxed regulatory agencies.[224] Further, trends in tort claims can provide important cues to regulators and legislators by generating collective data based on individualized or localized claims for relief.[225]

Perhaps the most effective work being done in the United States on the problem of cybersecurity is by state and federal regulators such as the FTC and state attorneys general. For years, scholars, advocates, and even entities in the technology industry have been calling for an increased regulatory role in this space, including recommendations for the creation of a separate federal agency to specifically address and enforce regulations in cybersecurity related issues.[226] The Biden administration's 2023 National Cybersecurity Strategy explicitly seeks new regulatory authority

---

224 George L. Priest, *The Invention of Enterprise Liability: A Critical History of the Intellectual Foundations of Modern Tort Law*, 14 J. LEGAL STUD. 461, 519 (1985) ("Enterprise liability theory in contrast appointed the judge an agent of the modern state. Negligence and warranty law were by their terms addressed solely to the one specific incident of product use before the court. Enterprise liability theory, in contrast, charged the judge to internalize costs and distribute risks. Enterprise liability theory also allowed judges to join the effort to aid the poor. Indeed, the theory conceived of courts as possessing unique powers to achieve these ends in comparison to alternative branches of government. Massive legislation would be required to aid, in any equivalent way, every poor person in every product purchase. The internalization and risk distribution powers enabled courts to adjust production decisions in the economy in ways that the legislative branch could approximate only through tax legislation and that the executive branch could not approximate at all. In contrast to negligence and warranty law, enterprise liability theory incorporates a conception of the judicial role in a complex governing state.").

225 *See, e.g.*, Roger J. Traynor, *The Ways and Meanings of Defective Products and Strict Liability*, 32 TENN. L. REV. 363, 366, 369–70, 375–76 (1965); Priest, *supra* note 224.

226 *See, e.g.*, Derek E. Bambauer, *Cybersecurity for Idiots*, 106 MINN. L. REV. 172, 174–76 (2021); David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. L. REV. 287 (2014); PAUL NICHOLAS & KAJA CIGLIC, MICROSOFT, BUILDING AN EFFECTIVE NATIONAL CYBERSECURITY AGENCY (2017), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE1RlTy [https://perma.cc/M58V-CNPZ]; Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503 (2012); Ido Kilovaty, *Cybersecuring the Pipeline*, 60 HOUS. L. REV. 605 (2023); David Thaw, *Data Breach (Regulatory) Effects*, 2015 CARDOZO L. REV. DE NOVO 151; Scott J. Shackelford & Scott Russell, *Above the Cloud: Enhancing Cybersecurity in the Aerospace Sector*, 10 F.I.U. L. REV. 635 (2015).

to "create a level playing field," "ensure that necessary investments in cybersecurity are incentivized," and "set[] new cybersecurity requirements" in order to defend critical infrastructure from cyberattacks.[227]

The concept of reasonableness is everywhere in regulatory theory and practice. When, for example, a federal regulation is genuinely ambiguous and could be reasonably read in more than one way in certain contexts, courts will defer to that agency's own reasonable interpretation of its own ambiguous regulations.[228] This doctrine is distinct from the judicial deference formerly given to an agency's interpretations of congressional statutes, which also rested on a foundation of reasonableness.[229] Reasonableness standards also play an important role in enforcement decisions. Courts may adjudicate enforcement actions by examining whether those being regulated have made reasonable efforts to comply with their regulatory obligations or if their actions allow the inference of a reasonable chance of future regulatory violations.[230]

When considering how existing regulations can apply to establishing a baseline for reasonable cybersecurity, we might well look to negligence per se as a model. Negligence per se claims generally rest on the belief that a common law basis should exist in circumstances where there already exist criminal or regulatory statutes that address those circumstances, such that those existing statutes can provide courts with the appropriate rule to establish common law liability.[231] Some argue that the use of negligence per se can overshadow the more appropriate application of case-by-case analyses of reasonableness, as it forces courts

---

227 WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY (2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [https://perma.cc/XF66-3RBP].

228 *See* Auer v. Robbins, 519 U.S. 452 (1997); *see also* Skidmore v. Swift & Co., 323 U.S. 134 (1944). Given the U.S. Supreme Court's rulings across several administrative law cases, scholars agree that the holding in *Auer* may be overruled in future terms. Thomas E. Nielsen & Krista A. Stapleford, *What* Loper Bright *Might Portend for* Auer *Deference*, HARV. L. REV.: BLOG (July 5, 2024), https://harvardlawreview.org/blog/2024/07/what-loper-bright-might-portend-for-auer-deference [https://perma.cc/74JS-NW8A]; Chad Squitieri, Auer *After* Loper Bright, YALE J. ON REG. (Oct. 15, 2024), https://www.yalejreg.com/nc/auer-after-loper-bright-by-chad-squitieri [https://perma.cc/M389-2CPW].

229 *See* Chevron U.S.A. Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837 (1984), *overruled by* Loper Bright Enters. v. Raimondo, 603 U.S. 639 (2024).

230 *See, e.g.*, *In re* N.J. State Funeral Dirs. Ass'n, 48 A.3d 391, 399 (N.J. Super. Ct. 2012); Fed. Trade Comm'n v. Neiswonger, 494 F. Supp. 2d 1067, 1080–81 (E.D. Mo. 2007) (providing to escape liability for civil contempt, defendant bears the burden of showing, inter alia, that they "made in good faith all reasonable efforts to comply" with the regulation in question); Amoco Oil Co. v. EPA, 543 F.2d 270, 274 (D.C. Cir. 1976); United States v. Lane Labs-USA, Inc., 324 F. Supp. 2d 547, 571–72 (D. N.J. 2004); Appalachian Power Co. v. Train, 620 F.2d 1040, 1046 (4th Cir. 1980).

231 *See, e.g.*, Miller v. City of Portland, 604 P.2d 1261, 1264 (Or. 1980).

to follow a more rigid standard based on statutory language.[232] But there are strong arguments that a model based on, but not necessarily identical with, negligence per se could both establish a "regulatory floor" upon which reasonable cybersecurity could be based, and this floor would be based on the kinds of expertise necessary to best assess what should and should not be considered reasonable in this context.[233]

Conversely, a common law basis for reasonable cybersecurity could help inform legislators and regulators in ways that result in better data security regulations as well as more effective rulemaking and enforcement of those rules. For the purposes of this Article, however, the role of reasonableness in a regulatory context is perhaps most useful in two quite different areas, the application of best available technology regulatory language, and the effects of applicable regulations on tort liability.[234]

A potentially useful tool from within the regulatory context—one that could extend beyond this context into civil liability for cybersecurity failures—is that of the "best available" and "best practicable" technology standards that have been adopted by the Environmental Protection Agency (EPA) in their rulemaking and enforcement of the Clean Air Act and Clean Water Act (CWA).[235] The rulemaking and subsequent caselaw articulating and interpreting these standards provides an apt platform upon which we could establish baselines of reasonable cybersecurity outside the regulatory context.

The notion of a technology-based standard for environmental regulation originated as a congressional response to the failings of earlier regulations that required states to adopt water quality standards for all interstate waters to "protect the public health or welfare [and] enhance the quality of water."[236] These standards were meant to set a maximum level of pollution for the safety of drinking, fishing, or otherwise using a

---

232 *See, e.g.*, Barry L. Johnson, *Why Negligence Per Se Should Be Abandoned*, 20 N.Y.U. J.L. & PUB. POL'Y 247, 249 (2017).

233 *See, e.g.*, Derek E. Bambauer, *Cybersecurity for Idiots*, 106 MINN. L. REV. HEADNOTES 172, 175–76 (2021).

234 *See supra* Section I.A.

235 *See* 42 U.S.C. § 7475(a)(4); 33 U.S.C. § 1326(b); 33 U.S.C. § 1311(b)(1)(A).

236 33 U.S.C. § 1313(c)(2)(A). Congress rejected this approach in 1971. *See* S. COMM. ON PUB. WORKS, FEDERAL WATER POLLUTION CONTROL ACT AMENDMENTS OF 1971, S. REP. NO. 92-414, at 4–5 (1971), *reprinted in* 1972 U.S.C.C.A.N. 3668, 3671; *see also* Weyerhaeuser v. Costle, 590 F.2d 1011, 1042 n.45 (D.C. Cir. 1978) (describing history of water quality regulatory acts and citing various earlier law review articles regarding the same); William L. Andreen, *The Evolution of Water Pollution Control in the United States—State, Local, and Federal Efforts, 1789–1972: Part I*, 22 STAN. ENV'T L.J. 145, 189–200 (2003).

waterway, but very few states moved to apply such standards.[237] When they were adopted, the regulations did not contain specific limits on pollution for individual dischargers, constraining regulators to enforcement only following a showing that a discharger violated the water quality standard, a complicated process that discouraged enforcement.[238]

To address these issues, Congress moved away from a health-based methodology, and passed the Federal Water Pollution Control Act Amendments in 1972, authorizing the EPA to set technology-based regulations for discharged pollutants from existing sources.[239] This Act directed the EPA to gather and study industry data to determine if pollution control technologies were available.[240] Applying the results of these studies, the EPA was charged with creating technology-based standards customized by the types of pollutant and category of discharger. Over the next few years, the EPA moved completely to a technology-based approach to pollution control.[241]

The 1977 CWA gave the EPA the authority to establish federal standards regulating the direct and indirect discharge of pollutants into the waters of the United States.[242] The Act requires direct dischargers of pollutants to comply with technology-based pollutant regulations that would, over time, become increasingly strict over stages.[243] The first stage ordered all direct dischargers to comply with pollutant limits through the application of the "best practicable control technology ('BPT') presently available" by July 1, 1977.[244] The second stage ordered all direct dischargers to meet a more stringent standard, the "best conventional

---

237 *See* S. REP. NO. 92-414, at 4–5 (1971), *reprinted in* 1972 U.S.C.C.A.N. 3668, 3671. (observing that many states did not have standards even after more than four years following the Act).

238 *See generally* P.D. Reed, *Industry Effluent Limitations Program in Disarray as Congress Prepares for Debate on Water Act Amendments*, 12 ENV'T L. REP. 10033 (1982). A 1972 Senate Report noted an "almost total lack of enforcement" of the water quality standards. S. REP. NO. 92-414, at 5 (1971), *reprinted in* 1972 U.S.C.C.A.N. 3668, 3671. It also referred to the "great difficulty associated with establishing reliable and enforceable precise effluent limitations on the basis of a given stream quality," and observed that the standards "often cannot be translated into effluent limitations—defendable in court tests, because of the imprecision of models for water quality and the effects of effluents in most waters." *Id.* at 7–8.

239 Federal Water Pollution Control Act Amendments of 1972, Pub. L. No. 92-500, 86 Stat. 816 (codified at 33 U.S.C. §§ 1251–1387).

240 *See* D. Bruce La Pierre, *Technology-Forcing and Federal Environmental Protection Statutes*, 62 IOWA L. REV. 771, 810–11 (1977).

241 33 U.S.C. § 1311(b)(2)(A), (b)(2)(C)–(b)(2)(D).

242 Pub. L. No. 95-217 § 42, 91 Stat. 1566, 1583 (1977) (codified as amended at 33 U.S.C. § 1311(b) (1982)).

243 33 U.S.C. §§ 1311(b), 1314(b).

244 *Id.* § 1314(b).

pollution control technology" (BCT) by March 31, 1989.[245] This latter stage also required that, by this same date, direct dischargers of toxic pollutants must comply with an even stricter limit based on the "best available technology economically achievable" (BAT).[246]

Congress authorized the EPA to determine the BPT, BCT, and BAT standards and promulgate them in regulations necessary to meet the various classes of pollutant dischargers, requiring the agency to consider a number of factors including cost. It is noteworthy for this Article's purposes, however, that cost was not necessarily the primary factor for consideration, and was to be given less weight both for pollutants that were more harmful to the environment as well as for discharge facilities that had not yet been constructed.[247] In fact, for new direct discharge sources constructed after the promulgation of these rules, an even more exacting standard, the "best available demonstrated control technology," would be defined and applied by the EPA.[248]

In *Chemical Manufacturers Association v. United States Environmental Protection Agency*, the U.S. Court of Appeals for the Fifth Circuit first reviewed these promulgated technology standards in the face of an industry challenge to their reasonableness.[249] With respect to the EPA's BPT standards, the court agreed with the agency's economic justifications, rejecting the industry group's tests for economic reasonableness as well as other technical challenges to the standard.[250] The court also accepted the EPA's basis for its BAT standard, and even held that the standard "may be too lenient."[251] Similar challenges to the BAT standards arose and were questioned as to their application to certain categories of industries, such as petroleum mining. In *American Petroleum Institute v. United States Environmental Protection Agency*, the Fifth Circuit once again reviewed EPA regulations, including a challenge to the BAT standard as it applied to discharge resulting from oil drilling.[252] The CWA also required that the EPA create and apply these standards to cooling water intake structures on power plants, calling for EPA rulemaking that "the location, design, construction, and capacity of cooling water intake structures reflect the best technology available for minimizing adverse environmental impact."[253]

---

245 *Id.*

246 *Id.* § 1311(b)(2)(A).

247 Chem. Mfrs. Ass'n v. U.S. EPA, 870 F.2d 177, 196 (5th Cir. 1989).

248 33 U.S.C. § 1316.

249 *Chem. Mfrs. Ass'n*, 870 F.2d at 196.

250 *Id.* at 204–24.

251 *Id.* at 227–28, 230–36.

252 858 F.2d 261 (5th Cir. 1988).

253 33 U.S.C. § 1326(b).

Given the complexities behind the analyses of assessing liability for the pollution of air and water, it is reasonable to believe that creating analogous standards for cybersecurity best practices is achievable. For example, the EPA rule requiring the "best available technology economically achievable" applies to "toxic" pollutants, which are particularly harmful or even fatal in small amounts.[254] Courts have upheld these rules as aligning with congressional intent that limitations on such pollutants should be "based on the performance of the single best-performing plant in an industrial field."[255] Given the levels of controversy such "best available technology" rules can create, if these standards can be upheld in environmental cases, similar standards can be found for cases of cybersecurity failure. Further, like the differing standards the EPA has created based on time elapsed and the severity of the pollutants involved, a regulatory agency can just as well draft rules to reflect similar differences in cybersecurity contexts.

III. DERIVING A TEST FOR REASONABLE CYBERSECURITY

Using the various examples of reasonableness standards described above, along with the motivations behind their uses, a model for a reasonable cybersecurity standard can begin to take shape. In addition, as Scott Shackelford, Anne Boustead, and Christos Makridis point out, states have made much more progress than the federal government in their efforts to create accountability for cybersecurity failures.[256] They also agree with the historical evolution of reasonableness standards that have been rooted in their flexibility depending on the context of their application, as well as the necessity for such standards to evolve as circumstances change over time.[257]

Without some kind of real risk of liability for poor data security practices, it is unlikely that we will see any significant improvement in computer and network security. It is a well-accepted principle in economics that incentives matter, and this principle has been applied widely in acknowledgement of its general relevance. Because good data security practices can be expensive, companies will minimize these costs where they can, exercising risk management principles as they would apply anywhere else in their budgets. If the costs associated with cybersecurity failures are low, the justification for expenditures to

254 *See* 33 U.S.C. §§ 1326(b), 1311(b)(2)(A)(i); 40 C.F.R. §§ 414.91, 414.101.

255 *See, e.g.*, *Chem. Mfrs. Ass'n*, 870 F.2d 177, 226 (5th Cir. 1989).

256 *See* Scott J. Shackelford, Anne Boustead & Christos Makridis, *Defining "Reasonable" Cybersecurity: Lessons from the States*, 25 YALE J.L. TECH. 86, 104–05 (2023).

257 *Id.* at 94–95; *see also* Schlag, *supra* note 44 and accompanying text.

alleviate those risks is also low. And what is therefore considered reasonable cybersecurity will only set the bar as high as necessary to account for these low costs—the incentives to improve cybersecurity are insufficient to address external harms.

A proposed solution to this problem has been to look to industry best practices for what is reasonable. But by themselves, these practices most often result in a kind of checklist culture of security, where it is more important to satisfy audit requirements than address specific cybersecurity needs, even if those requirements end up costing more with little actual data security to show for it.[258] Bruce Schneier illustrates this problem well using the concept of firewalls, which became ubiquitous not because of their effectiveness in providing data security (since many are poorly installed and maintained), but because they became an industry best practice, and therefore another box to check on the security audit.[259] A useful standard for cybersecurity reasonableness must therefore create the kinds of incentives that move organizations toward effective security practices, relying on bases for reasonableness that are more holistic in nature.[260]

But the complex nature of cybersecurity necessitates incentives that contain some degree of flexibility, as bright-line rules will yield many of the same perverse incentives as the checklist culture of security illustrated above. The flexible standards versus bright-line rules debate has been ongoing between legal scholars for decades.[261] Rules promote a formal kind of equality and predictability, whereas standards, in their flexibility, can be ambiguous and difficult to predict whether and how they might apply to one's actions. But standards also allow decision-makers to take into account all of the relevant facts of each case, adding a kind of fairness

---

258 *See, e.g.*, Julie Haney & Wayne Lutters, *Security Awareness Training for the Workforce: Moving Beyond "Check-the-Box" Compliance*, 53 COMPUT. (LONG BEACH CAL.) 91 (2020); *see also* Claas Lorenz, Vera Clemens, Max Schrötter & Bettina Schnor, *Continuous Verification of Network Security Compliance*, IEEE TRANSACTIONS ON NETWORK & SERV. MGMT, Dec. 2021 (proposing an alternate means of conducting security assurance reviews effectively).

259 Bruce Schneier, *Liability and Security*, CRYPTO-GRAM (Apr. 15, 2002), https://www.schneier.com/crypto-gram/archives/2002/0415.html#6 [https://perma.cc/6C44-XFVF].

260 It is worth noting two things here. First, industry best practices should of course not be ignored when developing a standard of cybersecurity reasonableness. Second, industry best practices, if updated, can become a kind of positive feedback loop, considering the changes in cybersecurity reasonableness standards over time as technologies and uses of those technologies continue to evolve.

261 *See, e.g.*, H.L.A. HART, THE CONCEPT OF LAW 121–37 (1961); Duncan Kennedy, *Form and Substance in Private Law Adjudication*, 89 HARV. L. REV. 1685, 1693, 1776–77 (1976); Kathleen M. Sullivan, *The Supreme Court 1991 Term: Foreword: The Justices of Rules and Standards*, 106 HARV. L. REV. 22, 57–69 (1992); *see also supra* Section I.A; Schlag, *supra* note 44 and accompanying text.

to proceedings that a rules-based order might lack. Both approaches can be appropriate in different contexts, but the complexity and constantly changing nature of cybersecurity factors and circumstances make a flexible reasonableness standard more useful in creating the right kinds of incentives necessary for better data security.

A. *Applying Cybersecurity Reasonableness Standards by Context*

The technologies and their uses we mean to protect will not only differ depending on how, why, and by whom they are used, but will also bear differing relationships to the parties that may be involved in and around their use. That is, technology manufacturers, resellers, and end users will all differ in the ways in which they interact with these technologies. Even between technology end users, there is a broad spectrum of sophistication and capability that will necessarily play a significant role in what might be considered reasonable in a cybersecurity context. How can we best, then, fairly apply a cybersecurity reasonableness standard to parties whose roles, contexts, and backgrounds can vary as widely as the different ways we use technologies?

Courts have long struggled with the question of applying standards of conduct in a way that applies rules of liability equitably. What standard of conduct, for example, should apply to drivers approaching a railroad crossing?[262] How should a court assess performance in good faith by parties to a contract?[263] How should a court decide what an appropriate use of force by a police officer should be?[264] Or when faced with questions of injury relating to the disclosure of medical risks, should we look to the actions of the doctor or the patient when assessing liability?[265] While all of these questions assume some kind of standard based on what is reasonable, they also encompass a wide array of human interactions by people with widely differing amounts of responsibility, experience, and

---

262 *Compare* Baltimore & O.R.R. Co. v. Goodman, 275 U.S. 66, 69–70 (1927) (arguing for a clear rule that drivers approaching a railroad crossing "knows that he goes to a place where he will be killed if a train comes upon him" and therefore "[h]e knows that he must stop for the train not the train stop for him"), *with* Pokora v. Wabash Ry. Co., 292 U.S. 98, 101–02 (1934) (arguing that drivers in such situations do not have such a duty to stop at the crossing, but should instead use "reasonable caution," arguing for a standard rather than a bright-line rule).

263 *See, e.g.*, Steven J. Burton, *Breach of Contract and the Common Law Duty to Perform in Good Faith*, 94 HARV. L. REV. 369, 390–91 (1980).

264 *See, e.g.*, Graham v. Connor, 490 U.S. 386, 396 (1989) (holding that Fourth Amendment reasonableness "must be judged from the perspective of a reasonable officer on the scene, rather than with the 20/20 vision of hindsight").

265 More specifically, how do we apply standards of the "reasonable physician" and the "reasonable patient"?

training. It would therefore be unfair—and perhaps impossible—to adjudicate all of these questions of liability based on one reasonableness standard, but instead we must consider the relevant contexts in which these people interacted.

When we consider questions of liability where issues of cybersecurity play a role, we must consider not only the parties' actions, but also their individual contexts and relevant roles they played. This is not, in itself, unusual. We go through such exercises in non-cyber contexts regularly, and so it is therefore useful to look to some examples of similar approaches for guidance. For organizational purposes, this Article has grouped its historical approaches to defining a reasonableness standard by the contextual circumstances each method means to adjust for: information imbalances, differences in sophistication and capabilities of the parties, differences in perceptions or values, and differences in power and responsibilities.[266]

1. Accounting for Severity of Resulting Injury

The risks associated with societal interactions are unavoidable, and our legal systems of liability try to account for this fact.[267] But the calculus associated with such approaches often shows boundary condition effects when the foreseeable injuries associated with such activities become increasingly severe. Our rules have accommodated for these uncomfortable effects by looking not to an individual's injuries, but attempt instead to evaluate effects at a societal level—are we generally better or worse off when we consider both the activity and its real and potential harms?

The Restatement (Third) of Torts addresses this issue directly, stating that when evaluating negligence claims, the "[p]rimary factors to consider in ascertaining whether the person's conduct lacks reasonable care are the foreseeable likelihood that the person's conduct will result in harm, the *foreseeable severity of any harm that may ensue*, and the burden of precautions to eliminate or reduce the risk of harm."[268] This

---

266 This taxonomy is not meant as the only possible way to think about reasonableness theories. For example, other methods may organize theories according to accepted convention and means. *See, e.g.*, Kevin P. Tobia, *How People Judge What is Reasonable*, 70 ALA. L. REV. 293, 312–15 (2018).

267 Martin Stone, *On the Idea of Private Law*, 9 CAN. J.L. & JURIS. 235, 259 (1996) ("[T]he situation in which one person suffers through the doing of another . . . has a natural saliency for human beings. It is bound to figure in the most basic thinking about what sorts of happenings can be controlled, and related to this, it produces such natural psychological responses as resentment and revenge.").

268 RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 3 (AM. L. INST. 2010) (emphasis added).

means we are frequently asked to consider gains that may outweigh severe harms or even death, a prospect that can sometimes verge on the amoral. If the potential severity of injury reaches unacceptable levels—the definition of unacceptable being subject to disagreement—we have adjusted our legal systems to compensate for this, even going so far as to impose strict liability in limited circumstances.[269]

2. Accounting for Information Imbalances

There are many common situations in everyday life where differences in information and uncertainty can create unfair relationships or transactions that may require adjustments to standards of what is reasonable under the circumstances. For example, markets for automobiles, insurance, employment, and credit for underdeveloped nations are vulnerable to information imbalances between buyer and seller, where the seller may use their superior information position to reduce the quality—and thus their own costs—of a product while still charging a premium for it, what George Akerlof called the "Lemons Principle."[270] This result is a market failure, and legal means to correct for this failure will ascribe different standards of reasonableness to the buyer (who lacks necessary information) and the seller.

In a regulatory context, for example, the Americans with Disabilities Act (ADA) forbids covered entities from discriminating against people with disabilities, including a requirement to make "reasonable accommodations" for these disabilities.[271] In order to arrive at what is reasonable under the ADA and the circumstances, employers and employees are required by courts to engage in a "good faith back-and-forth process between the employer and the employee, with the goal of identifying the employee's precise limitations and attempting to find reasonable accommodation for those limitations."[272] Courts considering ADA reasonable accommodations cases see these engagements as necessary, because the parties involved each have information the others do not have but require, and this kind of good

---

269 *See, e.g.*, RESTATEMENT (FIRST) OF TORTS § 339 (AM. L. INST. 1934) (expanding the scope of landlord liability by recognizing that landowners owed children a heightened duty of care when the risk of harm far exceeded the utility to the landowner from the dangerous condition); RESTATEMENT (SECOND) OF TORTS § 402A (AM. L. INST. 1965) (applying heightened liability for the sale and manufacture of an unreasonably dangerous product sold in a defective condition).

270 *See* George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488 (1970).

271 42 U.S.C. § 12112(a), (b)(5)(A).

272 *See, e.g.*, Aubrey v. Koppes, 975 F.3d 995, 1009 (10th Cir. 2020).

faith interaction is the best way to arrive at what is reasonable under the circumstances.[273]

In a cybersecurity context, this category should adjust reasonableness standards based on the often-severe information asymmetries between technology manufacturers or resellers and the average consumer who often has little knowledge of the complexities of the software or hardware they are purchasing. This problem exists across many consumer choices, where the products are too complex, their workings too obfuscated, or their use so ubiquitous that the consumer does not care to know any more than they have to about the product's inner functions. We see this in the example of the automotive industry. Cars are increasingly complex machines, as much computer as they are automobile, to the point where most consumers cannot know the details of their operation beyond what is needed to drive them. This is a significant information asymmetry between manufacturer and consumer. But auto manufacturers now regularly advertise the details of their safety features in order to attract consumers who just will not buy an unsafe car. This was not always the case—the market changed when government regulations were introduced to require cars to all have certain safety and environmental components, creating a new axis of competition for manufacturers that ultimately benefited the consumer. Reasonableness standards for cybersecurity could do the same for the technologies we regularly purchase and depend upon.

3. Accounting for Sophistication and Capability Differences

This category is similar in scope to the previous category, in that it considers the differing information positions of the parties, but rather than focus solely on the immediate facts of the case, reasonableness adjustments in this category consider the levels of sophistication, experience, and capability the parties maintain. A key difference between this category and the information asymmetry category is the fact that even sophisticated buyers and users of technology may sometimes fall victim to unfair circumstances due to information imbalances.[274]

For example, in cases of fraud, courts may limit some defenses of comparative fault if the plaintiff was incapable of making reasonable

---

273 Dansie v. Union Pac. R.R. Co., 42 F.4th 1184, 1193 (10th Cir. 2022).

274 *See, e.g.*, Nathan Alexander Sales, *Privatizing Cybersecurity*, 65 UCLA L. REV. 620, 644–45 (2018) (describing the power imbalances between buyers and sellers of software vulnerabilities, where those who discover these vulnerabilities, while knowledgeable, are often at a significant information disadvantage when dealing with large technology firms).

decisions due to incapacity or other structural factors.[275] When someone intentionally deceives another due to these factors, fraud actions will consider sophistication levels explicitly.[276] Similarly, contract law will explicitly change an understanding of reasonableness depending on the sophistication of the parties.[277] In cases considering a manufacturer's failure to warn about product dangers, courts lean on the manufacturer's sophistication regarding its own products when considering the reasonableness of their actions, but may also take into account whether the consumer themselves has a higher than average degree of sophistication or knowledge.[278] Legal frameworks meant to address the theft of trade secrets require that businesses take "reasonable measures" to keep such information secret, but courts will decide what is reasonable based on, inter alia, the sophistication and capabilities of the business.[279] Even the ethical rules lawyers apply to themselves take into account the sophistication of the user of legal services when deciding what "reasonable measures" might mean.[280]

Like the framings in these examples, situations involving cybersecurity should also consider the parties' sophistication and capabilities when it comes to deciding what is reasonable. When the average consumer purchases a smartphone, they are likely neither capable nor particularly interested in understanding the component-level details of the advanced hardware and software that the phone comprises. The relationship between the phone's manufacturer and that consumer is quite different than the relationship between a software manufacturer selling their product to a hardware manufacturer who intends to sell their bundled products as a package. In these scenarios, the specific imbalances or parities between the parties' knowledge and capabilities should be fully

---

275 *See, e.g.*, Ellen M. Bublick, *Comparative Fault to the Limits*, 56 VAND. L. REV. 977, 998 (2003).

276 *See, e.g.*, Edward J. Balleisen, *America's Anti-Fraud Ecosystem and the Problem of Social Trust: Perspectives from Legal Practitioners*, 118 NW. U. L. REV. 51, 53–54 (2023).

277 *See, e.g.*, Mark P. Gergen, *A Defense of Judicial Reconstruction of Contracts*, 71 IND. L.J. 45 (1995) ("The doctrines on impracticability[] [and] mistake[] share a feature that is unusual in contract law. They give courts the power to excuse or modify terms in contracts between sophisticated parties who bargained over terms of the contract with equal power and information."); Benjamin E. Hermalin & Michael L. Katz, *Judicial Modification of Contracts Between Sophisticated Parties: A More Complete View of Incomplete Contracts and Their Breach*, 9 J.L. ECON. & ORG. 230, 233 (1993); Alan Schwartz & Robert E. Scott, *Contract Theory and the Limits of Contract Law*, 113 YALE L.J. 541, 547 (2003).

278 *See, e.g.*, William G. Adamson & Adam S. Levy, *Duty to Warn for Products Used in the Industrial Workplace—"Sophisticated User" and "Learned Intermediary" Defenses*, 65 PA. B. ASS'N Q. 26 (1994).

279 *See, e.g.*, Steve Sozio & Dave Drab, *Economic Espionage in the New Millenium*, 48 FED. LAW. 24, 25–26 (2001).

280 *See, e.g.*, Jennifer M. Pacella, *The Regulation of Lawyers in Compliance*, 95 WASH. L. REV. 947, 991 (2020).

accounted for when considering what is considered reasonable behavior regarding data security choices.

4. Accounting for Differences in Power and Responsibility

A notional basis for what we are to consider reasonable under the law is one of a "certain average of conduct" which is "necessary to the general welfare."[281] Note the difference between this standard and one that looks to model behavior or conduct we should all aspire towards. Reasonableness is largely descriptive rather than normative, a depiction of a kind of social median from which we measure the acceptability of—and potential liability for—actions.[282] But when significant differences in responsibility and power exist between parties, we adjust the averageness concept to correct for these differences and normalize what kinds of behavior should be considered reasonable under these circumstances. These adjustments can take a wide array of forms, as responsibility and power differentials show up in all sorts of ways.

For example, we adjust the reasonableness standard to account for those whose age or mental competence put them at a disadvantage with respect to others.[283] Courts look to the "reasonable police officer" standard when adjudicating use of force claims, both to account for the training and responsibility vested in the officer, but also the circumstances these officers can find themselves in.[284] The relationship between doctor and patient yields multiple reasonableness adjustments that must account for training, responsibility, power, and trust in healthcare scenarios.[285] We have applied "reasonable manufacturer"

---

281 OLIVER WENDELL HOLMES, JR., THE COMMON LAW 108–12 (1881).

282 *See supra* Part I.

283 *See, e.g.*, David E. Seidelson, *Reasonable Expectations and Subjective Standards in Negligence Law: The Minor, the Mentally Impaired, and the Mentally Incompetent*, 50 GEO. WASH. L. REV. 17, 20–21 (1981); J.D.B. v. North Carolina, 564 U.S. 261, 271–72 (2011) ("In some circumstances, a child's age 'would have affected how a reasonable person' in the suspect's position 'would perceive his or her freedom to leave.' That is, a reasonable child subjected to police questioning will sometimes feel pressured to submit when a reasonable adult would feel free to go." (quoting Stansbury v. California 511 U.S. 318, 325 (1994))).

284 *See* Graham v. Connor, 490 U.S. 386, 396–97 (1989). This standard is controversial, however, due to its vagueness as well as the weight courts tend to attribute to government interests and police testimony regarding the facts of the case.

285 We have imposed a standard of reasonable care on doctors, which goes beyond the negligence standards we normally apply under a reasonable person standard, in order to account for the "degree of care, skill, and proficiency" expected of physicians in good standing in the medical profession. Vergara by Vergara v. Doan, 593 N.E.2d 185, 186–87 (Ind. 1992); *see also* Beadling v. Sirotta, 197 A.2d 857, 860 (N.J. 1964). We also have a specific reasonableness standard when

standards to questions of post-sale duties to warn about product hazards, and we have also created defenses to these claims based on a "sophisticated user" standard.[286] Within this vein, such failure to warn cases can rely upon a "reasonably prudent manufacturer" standard if they are argued within a negligence context, but such reasonableness arguments do not apply under strict liability principles.[287]

Technology manufacturers and resellers are often in positions of power or responsibility over their consumers and users. This relationship can be illustrated through the evolution of the automobile industry. From their introduction to U.S. markets through the 1950s, cars were designed and marketed largely based on aesthetics, with relatively little thought given to safety concerns. When accidents did happen and people were injured, they faced significant difficulties when seeking relief in courts as automobile manufacturers often used disclaimers and waivers in contracts to avoid many warranty provisions and consequential damages.[288] Changes in regulations and tort law forced automobile manufacturers not only to make their vehicles safer, but also created a duty owed to their customers based on the responsibility inherent in the relationship, and allowed for liability when their products were unreasonably unsafe.[289] This same kind of power relationship between technology manufacturers and platforms and their consumers should require similar consideration.[290]

---

judging the defectiveness of prescription drugs, holding that a reasonable medical professional would not prescribe defective products. *See* RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 6(C) (1998).

286 *See, e.g.*, Johnson v. Am. Standard, Inc., 179 P.3d 905 (Cal. 2008).

287 *See, e.g.*, Anderson v. Owens-Corning Fiberglass Corp., 810 P.2d 549, 559 (Cal. 1991).

288 *See, e.g.*, Henningsen v. Bloomfield Motors, Inc., 161 A.2d 69, 74 (N.J. 1960) (noting that the standard automobile sales contracts for Plymouth's automobiles included fine print disclaiming all "warranties, express or implied, made by either the dealer or the manufacturer on the motor vehicle, chassis, or parts furnished").

289 *See, e.g.*, Larsen v. Gen.l Motors Corp., 391 F.2d 495, 501–02 (8th Cir. 1968) ("Accepting, therefore, the principle that a manufacturer's duty of design and construction extends to producing a product that is reasonably fit for its intended use and free of hidden defects that could render it unsafe for such use, the issue narrows on the proper interpretation of 'intended use.' Automobiles are made for use on the roads and highways in transporting persons and cargo to and from various points. This intended use cannot be carried out without encountering in varying degrees the statistically proved hazard of injury-producing impacts of various types. The manufacturer should not be heard to say that it does not intend its product to be involved in any accident when it can easily foresee and when it knows that the probability over the life of its product is high, that it will be involved in some type of injury-producing accident.").

290 *See, e.g.*, Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553 (2005).

5. Accounting for Existence of Preexisting Norms or Standards

The existence of accepted community or industry norms or best practices are considered by courts when assessing what actions may or may not be considered reasonable under the circumstances. Decision-makers can find preexisting norms of considerable use, as it takes what might otherwise be an unrestricted inquiry into a party's reasonableness and provides something of a framing from which to proceed. This framing can range from advisory to something akin to a bright-line rule, where only a violation of a norm or best practice will qualify as unreasonable under the circumstances.[291] This Article recommends that a more balanced approach to norms and standards should be adopted in the cybersecurity context.

In medical malpractice cases, for example, what is considered reasonable may depend on the norms and standards within the medical community.[292] In the data security context, the FTC has often looked to industry standards and best practices when considering what is unfair or misleading. A company making claims (or inferences) that their products are secure, or their customers' data is protected by encryption, may run afoul of the FTC Act if their claims of security and encryption do not meet current technology industry standards.[293]

We might also consider regulatory norms, like the BAT and BPT standards applied by the EPA in the regulation of clean air and clean water.[294] The FTC would be a likely candidate for setting these norms, but it is not unforeseeable that other agencies could aid in this effort, in cooperation with industry stakeholders. Such a standard of consideration would likely present a kind of balancing test on its own, but any such "best available technology" test for cybersecurity should not give more weight to costs at the expense of the goal of reducing data security failures.

---

291 *See, e.g.*, Richard C. Ausness, *The Case for a "Strong" Regulatory Compliance Defense*, 55 MD. L. REV. 1210, 1221–23, 1265–67 (1996) (arguing that administrative cost savings will offset the negative effects in product safety).

292 *See, e.g.*, Chapel v. Allison, 785 P.2d 204, 207 (Mont. 1990) ("[T]his Court recognized that the defendant was a nationally board-certified orthopedic surgeon and had received comparable training and passed the same national board certification tests as all other board-certified orthopedic specialists in the nation. On that basis, this Court held that when a defendant in a medical negligence action was a board-certified specialist, his skill and learning would be measured by the 'skill and learning possessed by other doctors in good standing, practicing in the same speciality [sic] and who hold the same national board certification.' Thenceforth, board certified specialists in Montana would be subject to a national standard of care." (quoting Aasheim v. Humberger, 695 P.2d 824 (Mont. 1985))).

293 *See* Solove & Hartzog, *supra* note 8, at 636–37.

294 *See supra* Section II.E.

When considering industry norms or standards, however, it is important that this assessment is not conducted in a rote fashion. Just because a standard exists does not necessarily mean that it is a good standard. Consistency does not always yield quality, and existing standards that do not reflect what might otherwise be considered reasonable behavior in a contemporary context should be ignored, or even better, replaced. Further entrenching bad norms only serves to limit improvements upon reasonableness standards.

B. *A Cybersecurity Reasonableness Test*

While the concept of reasonableness can sometimes be a slippery one, we have generally done well in setting the parameters of the standard to fit the circumstances presented by the widely differing cases to which the standard is applied. In this vein, attempts by courts and lawmakers to ascertain just what reasonableness means in a cybersecurity context have been hit or miss, often looking for footholds from other cases that fail to take into account some of the unique factors presented by situations often difficult to describe in the physical terms we are most accustomed to.[295] A usable standard of cybersecurity reasonableness must, therefore, adopt where it can from the long lineage of reasonableness jurisprudence, and also adapt itself to the circumstances presented, even as those circumstances are bound to change as our technologies and their uses evolve. Additionally, a useful cybersecurity reasonableness standard should not be artificially limited only to certain parties, such as technology manufacturers, as the problem of data security is found across all technology uses and users.

To that end, this Article proposes a set of five factors to evaluate whether an actor's cybersecurity practices should be considered reasonable under the circumstances. These factors are meant to be taken together, but depending on the case, a decision-maker may find it prudent to put more weight on some factors over others. These factors are designed to account for the costs of failure, the likelihood of risk, the resources and capabilities of the actor, the role that actor takes within the context of the case, and the existence of accepted standards and practices applicable to the case. Evaluated collectively, these elements can be used to create a defensible basis for cybersecurity reasonableness.

---

295 *See* HERBERT A. SIMON, THE SCIENCES OF THE ARTIFICIAL 174 (3d ed. 1996) ("Much of the motivation for [the current burst of interest in complexity] is the growing need to understand and cope with some of the world's large-scale systems the environment, for one, the world-wide society that our species has created, for another, and organisms, for a third.").

1. What Are the Stakes of Failure?

Perhaps the most important aspect of any cybersecurity failure is an assessment of the actual costs, both actual and potential, of that failure. Because our use of computers extends from the most pedestrian to the most critical parts of our everyday lives, we cannot expect a cybersecurity reasonableness standard to apply rigidly to every scenario in which a data security failure can occur. A data breach that results in the exposure of customer email addresses should not resonate at the same risk frequency as one that results in loss of control of a vehicle moving at high speeds on a busy highway.[296] The costs and inconvenience associated with a requirement to change passwords or purchase credit monitoring services are not the same costs that come with permanent heart damage caused by a software-controlled device during bypass surgery.[297] Accounting for the dangers posed by data security failures is a necessary element of any cybersecurity reasonableness analysis.

A full evaluation of this element should consider the wide range of potential harms that can stem from a data security failure. Courts have historically looked first to economic consequences, these being easiest to assess and remedy.[298] Economic harm from data security failures have also been historically common due to the fact that for the first decades of widespread computer use, their effects were largely limited to the nonphysical. But things have changed. It is entirely likely that software or hardware (or some combination of the two) can create real physical harms, and actors that operate in this space should be held to a reasonableness standard that accounts for these significant differences.[299] In addition to these more easily measurable harms, it is becoming increasingly evident that psychological, reputational, and societal harms can be just as damaging.[300]

---

296 *See, e.g.*, Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, WIRED (July 21, 2015, 6:00 AM), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway [https://perma.cc/WVJ3-3TRU].

297 *See* Singh v. Edwards Lifesciences Corp., 210 P.3d 337 (Wash. Ct. App. 2009).

298 In fact, harms beyond those that can be easily assessed, like economic losses and physical damage, can be seen by courts as insufficient to maintain Article III standing to bring the case. *See, e.g.*, Spokeo, Inc. v. Robins, 578 U.S. 330, 340–41 (2016) (the Court held that the Article III case or controversy requirement demands that justiciable cases must involve injuries that are "concrete," "real" and "not abstract," and "bare procedural violation[s]" do not satisfy this requirement).

299 *See, e.g.*, Choi, *supra* note 14.

300 *See, e.g.*, Eva Ignatuschtschenko, *Assessing Harm from Cyber Crime*, *in* THE OXFORD HANDBOOK OF SECURITY 128 (Paul Cornish ed., 2021) ("An understanding of the full spectrum of potential harm that can arise as a result of cyber crime is important in order, first, to detect and assess harm in all its manifestations. Even if one would be concerned only about the financial

When applying this factor, it is also critical not only to evaluate the magnitude of harm as applied individually, but to look to the potential scale of the harms that will often come with technology territory. For example, given the sheer number of people who use global computer systems, both for work as well as for play, an exploitable vulnerability that might otherwise be innocuous on a small network becomes orders of magnitude more significant if that same vulnerability exists on Facebook's, Target's, or the Industrial and Commercial Bank of China's systems.[301] To properly assess the weight of this element, it therefore becomes necessary to evaluate whether or not the circumstances amount to significant harm from a thousand tiny cuts.

2. What Is the Likelihood of Failure?

Any standard risk analysis must examine not only the costs associated with risks, but their probabilities, as well. It would make little sense to spend significant resources addressing risks with little to no likelihood that they will occur.[302] Applying this principle, a usable reasonable cybersecurity standard must allow the actor to derive their security decisions based in part on the foreseeable likelihood that any particular harm could arise from a data security failure. These probability calculations can be based on a number of factors, such as the attractiveness of the actor's systems as targets for attack, deterrence factors of existing systems, the value of the data held on the actor's

---

implications of cyber crime . . . the costs would amount to more than just the mere loss of money . . . .").

301 *See, e.g.*, Emma Bowman, *After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users*, NPR (Apr. 9, 2021, 11:58 PM), https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users [https://perma.cc/6HK5-2W6U] (describing the breadth of a data breach leaking data from 533 million Facebook users in 106 countries); Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015, 8:29 AM), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned [https://perma.cc/57XH-33GS] (describing a data breach involving millions of customer credit cards and debit cards); Arjun Kharpal, *China's ICBC, the World's Biggest Bank, Hit by Cyberattack That Reportedly Disrupted Treasury Markets*, CNBC (Nov. 10, 2023, 10:21 AM), https://www.cnbc.com/2023/11/10/icbc-the-worlds-biggest-bank-hit-by-ransomware-cyberattack.html [https://perma.cc/N9RC-GQWT] (describing the hack on the world's largest lender by assets and its effect on world financial markets).

302 The possible exception to this rule can occur when the magnitude of the costs associated with the risk are extraordinarily high, making such an occurrence catastrophic. *See, e.g.*, CLIFFORD WATSON, RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD), SEVERITY, AND LEVEL OF CONTROL, NASA: FOURTH INT'L ASS'N FOR THE ADVANCEMENT OF SPACE SAFETY (2010), https://ntrs.nasa.gov/api/citations/20110015694/downloads/20110015694.pdf [https://perma.cc/87W4-SJDY].

systems, and the marginal effect any particular measure might already have on the overall security of the system.[303]

For example, a small startup technology company considering the creation of a simple task management tool that only stores names, dates, and descriptions, would have to take security precautions to ensure data safety and reliability, but these actions would be limited by the relatively low likelihood that they would be targeted as well as the relatively low value of the data they held. If, however, that same company rapidly became successful, gained a larger customer base, and started storing more sensitive (and potentially valuable) data, such as locations, financial information, or other personally identifiable information, what might have been reasonable earlier is likely no longer reasonable due to the increased probability of cybersecurity failures due to attractiveness as a target and the potential failure of their systems to keep up with the risk.

We should be careful, however, that this component is not mistaken for an actor's assessment of the probability of *punishment* or *liability* for cybersecurity failures. This calculation, though a reality in a company's overall risk assessment analysis, is based on a kind of cybersecurity market failure, one that the existing system of regulation has (thus far) failed to address.[304] Relatedly, this probability calculation should also not include the kind of assessment of an actor's customer base that differentiates based on a customer's access to legal recourse. Analysis of risk based on a customer's ability to sue is another market failure, improperly addressed by the existing legal system.

3. What Are the Actor's Resources and Capabilities?

When deciding what is and is not reasonable cybersecurity, we must also consider the resources and capabilities of the actors involved in data security failures. This component relies on established criteria that are applied when reasonableness or appropriateness is to be evaluated by a court. These criteria often boil down to a choice between an objective standard, a subjective standard, or a combination of the two that takes into account some kind of objective interpretation of what a similarly situated actor would due under the circumstances, but leavens it by limiting that standard to what one would expect of that actor, given its resource and capability limits.[305] We should expect that the cybersecurity

303 *See generally* THE LAW AND ECONOMICS OF CYBERSECURITY (Mark F. Grady & Francesco Parisi eds., 2006).

304 *See* Vagle, *supra* note 18 (describing the negative externalities of cybersecurity vulnerabilities and the subsequent moral hazards that occur due to this market failure).

305 *See* discussion *supra* Section II.B.

decisions involved in a system and network designed and built to locally manage a small hardware store's books would look quite different from the security choices of a multinational business that collects and stores the personal and financial information of millions of customers.[306]

This element cannot exist in a vacuum, however. An actor's limited resources or capabilities should not excuse poor cybersecurity decisions if other factors, such as the stakes of failure and likelihood of failure, would warrant more robust security choices. If, for example, the small business is not a hardware store but a small law firm that is entrusted with the storage of highly sensitive client information, a full assessment of this component will need to weigh the cybersecurity risks associated with the firm's choice of business alongside their resources and capabilities. That is, being out of one's cybersecurity depth should not be seen as reasonable.

4. What Is the Actor's Cybersecurity Role?

This component is related to, but should be distinguished from, the resources and capabilities reasonableness component, as it is meant to focus the evaluator on the power relationships between the various actors in a cybersecurity failure case. These kinds of assessments of reasonableness can appear in cases where the relationship between the parties in the case are tightly coupled with the harms involved. For example, in cases of sexual harassment and assault, power dynamics play a very significant role, making assessments of reasonableness unfair unless those assessments also take into account the relationship between harasser and victim and the disparities in power between them.[307] The assessment of reasonable actors in cybersecurity failure cases needs to follow this model—it is difficult, if not impossible, to equitably assess reasonableness without understanding the roles these actors played and the relationships between them.

The importance of an actor's role and the power relationships that stem from it are most evident when one considers the technological and information gaps that exist not only between technology manufacturers and their users, but also between technology companies and the government bodies meant to regulate them. Mark Zuckerberg's well-known philosophy urging technology companies to "[m]ove fast and

306 *See, e.g.*, *supra* Part I (discussing Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015)).

307 *See, e.g.*, Jolynn Childers, *Is There a Place for a Reasonable Woman in the Law? A Discussion of Recent Developments in Hostile Environment Sexual Harassment*, 42 DUKE L.J. 854, 857–58 (1993).

break things"[308] has yielded all manner of externalizations of information risk, with some companies going as far as eschewing the (time consuming and expensive) steps necessary to ensure customer safety.[309] For most consumers, the devices and services they purchase and use are black boxes—there is no easy way for them to assess the upstream security choices made by technology manufacturers and resellers. By considering the role of an actor—Did they write software or build the technology? Did they design and deploy the network? Did they make the cost decisions related to their data security choices?—a decision-maker can properly assess what should be considered reasonable cybersecurity actions for that actor.

5. What Independent Security Standards and Practices Apply?

Finally, any useful assessment of cybersecurity reasonableness should take into consideration the industry security standards or best practices that best fit the circumstances of a data security failure case. By themselves, these standards and practices can be misleading, and even result in unnecessary costs and perverse incentives.[310] Taken within the context of the other four cybersecurity reasonableness components, however, these standards can provide a meaningful baseline upon which the other components can build.

When evaluating this component, it is important to consider some caveats. First, the standards applied must be relevant to the circumstances before the decision-maker. There are standards that apply to critical infrastructure that are not generally relevant to consumer devices. Some standards are better suited to horizontal considerations, such as those that apply to industrial automation and control environments, and some standards are better suited for vertical contexts, such as in healthcare,

---

308 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*, BUS. INSIDER (Oct. 1, 2009, 8:36 PM), https://www.businessinsider.com/mark-zuckerberg-innovation-2009-10 [https://perma.cc/ZX6Q-7TG3].

309 While not strictly a cybersecurity issue, the safety considerations of some of the early automobile-related technology companies have been shocking. Waymo executives saw redundant systems for steering and braking as unnecessary, that employees who were more deliberate due to risk aversion were "not moving fast enough," and even waving of security and safety issues altogether, characterized by a text message that simply read "Burn the village." *See* Sarah Jeong, *Uber's Former Head of Self-Driving Cars Put Safety Second*, VERGE (Mar. 20, 2018, 2:42 PM), https://www.theverge.com/2018/3/20/17144090/uber-car-accident-arizona-safety-anthony-levandowski-waymo [https://perma.cc/UA6J-7FVJ].

310 *See supra* note 259 and accompanying discussion.

finance, and education environments.[311] Relatedly, a set of standards or best practices might be too onerous in some circumstances. What might be considered best practices for protecting the electrical grid is likely expensive or unattainable for a social media company.[312] Finally, a decision-maker should consider the "meta-purpose" of the standards. That is, do the standards build a bridge, enabling companies to make better cybersecurity decisions, or do they create a moat, strengthening the market positions of big players at the expense of smaller competitors and consumers? A fulsome evaluation of these factors can give decision-makers a robust basis upon which to consider the reasonableness of cybersecurity actions.

CONCLUSION

The concept of reasonable cybersecurity has proven frustratingly elusive to courts, lawmakers, and businesses—how can we apply a standard that has appeared in all manner of cases and contexts over centuries of jurisprudence to technologies and their use cases that may have only come into existence in the past few years? The need for a flexible standard that is technically grounded, empirically precise, yet accessible enough to judges and juries so that it may be fairly applied has long been missing, a fact that becomes more problematic as our technology uses continue to evolve and grow at a pace that makes bright-line rules an impossibility. By examining the reasonableness landscape, taking from it relevant parts, we can arrange them to create a basis for a component-based test that fairly considers the relevant factors of security failures, is accessible to courts and legislatures, and is flexible enough to weather the cybersecurity challenges our technologies are sure to bring.

311 *See, e.g.*, Int'l Soc'y of Automation, *ISA/IEC 62443 Cybersecurity Series Designated as IEC Horizontal Standards*, INTECH, Dec. 2021, at 1, 43, https://www.isa.org/getmedia/35803378-d97a-403a-861c-83ca96fb0430/InTech-December-2021.pdf [https://perma.cc/3EBG-FMDC]; *How FINRA Serves Investors and Members*, FINRA, https://www.finra.org/about/what-we-do [https://perma.cc/P4B4-QZFD].

312 *See, e.g.*, Nelson Hastings, Jeffrey Marron & Michael Bartok, *Cybersecurity for Smart Grid Systems*, NAT'L INST. STANDARDS & TECH. (July 8, 2023), https://www.nist.gov/programs-projects/cybersecurity-smart-grid-systems [https://perma.cc/5CLQ-E32D].