Missouri Law Review

Volume 89 | Issue 1 Article 6

Winter 2024

Cancel Carte Blanche for the Information Industries: Federalizing U.C.C. Article 2.

Michael L. Rustad

Cancel Carte Blanche for the Information Industries: Federalizing U.C.C. Article 2.

Michael L. Rustad [*]

ABSTRACT

Warranty disclaimers, caps on damages, predispute mandatory arbitration, and anti-class action waivers constitute what I call, "no

---

[*] Michael L. Rustad, Ph.D., J.D., LL.M., is the Thomas F. Lambert Jr. Professor of Law and Co-Director of the Intellectual Property Law Concentration at Suffolk University Law School in Boston, Massachusetts. Professor Rustad clerked for the late Judge William E. Doyle of the 10th Circuit U.S. Court of Appeals in Denver, Colorado and served as an associate with the Boston law firm of Foley, Hoag, prior to becoming a law professor. He teaches courses in Sales and Leases, Payments Systems, Secured Transactions/Bankruptcy, International Sales Law, and Tort Law. He has taught international business law and commercial law in Hungary, Ireland, Mexico, and Sweden. He is a member of the American Law Institute Consultative Group on tort remedies, defamation and privacy, and intentional torts. Professor Rustad was the Hugh F. Culverhouse Visiting Distinguished Professor of Law, Stetson University Law School for 2009-2010. Professor Rustad has testified before both Houses of Congress and has authored three amicus briefs before the U.S. Supreme Court on the constitutionality of punitive damages. He is an elected member of the American Law Institute (ALI and belongs to the ALI Member Consultative Groups of the Restatement of the Law (Third) Torts and Principles of Software Contracts. Professor Rustad was elected as Chair of the Executive Committee of the American Association of Law Schools Section on Torts and Compensation Systems. In 2012, Professor Rustad organized and spoke at the AALS Torts & Compensation Section panel, entitled *Twenty-First Century Tort Theories: A New Audit of Civil Recourse Theory*. He selected the 2013 Recipient of the William L. Prosser Award, AALS Torts & Compensation Systems Section (July 2012) with Judge Guido Calabresi and Judge Richard Posner. Professor Rustad has also served as a Task Force Leader for the American Bar Association's Business Law Section on Information Licensing. His book, IN DEFENSE OF TORT LAW (NYU Press, 1981) co-authored with Thomas H. Koenig, is one of the most widely cited tort law scholarly works. His most recent books are the five volume treatise COMPUTER CONTRACTS: NEGOTIATING, DRAFTING (Matthew Bender, updated 2024), GLOBAL INFORMATION TECHNOLOGIES: ETHICS AND THE LAW (2d ed. 2023) (with Thomas H. Koenig) and GLOBAL INTERNET LAW HORNBOOK, HORNBOOK SERIES (West Acad. 4th ed. 2022). Professor Rustad has authored more than fifty law review articles and review essays in journals such as the *Northwestern Law Review*, *North Carolina Law Review*, *Wake Forest Law Review*, and the *University of Illinois Law Review*. His signature article on punitive damages in products liability was one of the top twenty most cited articles in the history of the *Iowa Law Review*. Trained as a sociologist, Professor Rustad's contribution to that

responsibility" or "rights foreclosure clauses" in computer contracts. This is the first empirical study of how the information industries, which include the 100 largest software companies and the 100 largest digital companies, deploy one-sided warranty disclaimers, caps on damages, and predispute mandatory arbitration clauses coupled with class action waivers to shift responsibility for defective software to the user communities. This gives the information industries carte blanche to release dangerously defective software without consequences. In their standard form contracts, the industries do whatever they wish by incorporating their designed terms and conditions. The software industry assert contractual rights without providing corresponding meaningful remedies for breach in their computer contracts. The net effect of these no responsibility clauses is to require users to waive their right to a judicial forum in favor of arbitration, where the stronger party is at a distinct advantage. Congress needs to enact a federal U.C.C. Article 2 reform that will invalidate no responsibility clauses, thus restoring mutuality in software license agreements.

field was his book, WOMEN IN KHAKI: THE AMERICAN ENLISTED WOMAN (Praeger Publishers, 1982). Professor Rustad and his wife, Chryss J. Knowles, live in Vermont and are devoted grandparents.

TABLE OF CONTENTS

I. INTRODUCTION

Software is America's third largest industry,[1] and it will continue to grow and evolve as Americans live increasingly digitally enabled lives. The injuries, damages, and losses caused by flawed software has progressively increased over the past quarter century. Warranty disclaimers, caps on damages, predispute mandatory arbitration, and anti-class action waivers constitute what I call, "no responsibility" or "rights foreclosure" clauses. U.S. courts routinely uphold one-sided warranty disclaimers, limitation of liability clauses that cap damages at a nominal amount, and predispute mandatory arbitration clauses coupled with anti-action waivers. No responsibility clauses give the information industries carte blanche to release buggy software without consequences. Currently, the software and digital industries can do whatever they wish, imposing their designed terms and conditions on all users. Unbalanced "take it or leave it" standard forms need to be amended to reflect the interests of all licensees. Retiring Congressman David Cicilline (D.R.I.) argued Washington has been "asleep at the switch" when it comes to managing the growing might of the American tech industry.[2] He said of his first antitrust investigation in fifty years that he:

> learned very clearly [the tech industry] were a monopoly, and they were using monopoly power to maintain their monopoly, and to grow them, and it was really hurting innovation, consumers, and small businesses.[3]

My article will show a parallel abuse of power by the world's largest software and digital companies which are weaponizing contract law, allowing them to shift their responsibility to pay the costs of defective software to the user communities. In March 2023, the Biden Administration issued a new National Cybersecurity Strategy, in which it called for, among other things, legal reforms for the industry to secure its software and be liable for security flaws in their products.[4]

---

[1] 1 COMPUTER CONTRACTS § 1.02 (2023) ("Software licensing is rapidly displacing sales and leases as the leading computer contracting method. Software shapes nearly every aspect of the American experience and has evolved as the third largest industry in America.").

[2] Nancy Scola, '*Every Step of the Way, They Underestimated Us*', POLITICO MAG. (May 31, 2023, 4:30 AM), https://www.politico.com/news/magazine/2023/05/31/david-cicilline-exit-interview-tech-00099264 [https://perma.cc/V73A-6R9J].

[3] *Id.*

[4] NATIONAL CYBERSECURITY STRATEGY, WHITE HOUSE 20–21 (March 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [https://perma.cc/X3K9-BYP6] ("We must begin to shift liability

This article argues that federalizing U.C.C. Article 2 is the most effective way to invalidate "no responsibility clauses" such as eliminating all implied warranties and limiting remedies to a nominal dollar amount in software licensing agreements and other computer contracts. Part I explains how defective software causes physical injury, loss of life, destruction of property, and financial losses. Defective software may not only cause computers to crash but enable state-sponsored cybercriminals and other bad actors to misappropriate valuable data and trade secrets. Glitches in software threaten national security and the well-being of the government, private infrastructure, corporations, non-profit organizations, consumers and the general public.

Part II describes how Microsoft, the largest software company in the world, deploys no responsibility clauses in its standard form license agreements. Microsoft uses contract law to shift its responsibility for marketing software with known vulnerabilities to the user community. Next, Part II includes an empirical study of how the 100 largest software companies and the 100 largest digital companies also deploy "no responsibility" clauses to shift the costs and consequences of defective software to users. The overwhelming finding is that the information industry follows Microsoft's example in disclaiming all warranties, capping damages to a nominal amount and imposing arbitration coupled with anti-class action waivers.

Part III critically evaluates four tort law alternatives to address the software liability crisis: (1) A special purpose (*sui generis)* tort law statute; (2) recognizing computer malpractices; (3) strict products liability for defective software; and (4) recognition of a new negligent enablement of cybercrime tort. I conclude that there is no tactical tort solution to the software crisis. There are two major problems to making tort work for defective software. First, the Economic Loss Doctrine ("ELD") adopted by a majority of jurisdictions in the United States precludes recovery in tort, where the only damages are that the software does not function as designed.[5] The second problem is that the plaintiffs' recovery is stymied

---

onto those entities that fail to take reasonable precautions to secure their software while recognizing that even the most advanced software security programs cannot prevent all vulnerabilities. Companies that make software must have the freedom to innovate, but they must also be held liable when they fail to live up to the duty of care they owe consumers.").

[5] Jannarone v. Sunpower Corp., Civ. No. 18-9612, 2019 WL 4058981, at *8 (D.N.J. Aug. 28, 2019) ("The economic loss doctrine prohibits plaintiffs from recovering tort economic losses to which their entitlement only flows from a contract" (citation omitted)); *see also* Hodell-Natco Indus., Inc. v. SAP Am., Inc., No. 1:08 CV 02755, 2011 WL 2174365, at *6 (N.D. Ohio, June 2, 2011) (holding that plaintiff's negligence claim was barred under the economic loss rule because the plaintiff was seeking purely economic losses associated with defendant's breach of contract for software services).

by tort reforms such as hard caps on damages. The second problem is that rights foreclosure clauses in software contracts have undermined the functioning of the civil justice system.[6]

Part IV argues that revising U.C.C. Article 2, rather than a tort law solution, is the most efficient way to address defective software. My proposal is for Congress to enact a federal statute amending U.C.C. Article 2 nationwide to invalidate disclaimers of implied warranties, caps on damages, predispute mandatory arbitration clauses and anti-class action waivers. This would not be a radical or unprecedented step. In 1975, Congress, with bipartisan support, federalized U.C.C. warranty labels and consumer disclosures to make warranties on consumer products more readily understood and enforceable. The impact of reforming U.C.C. Article 2 is that plaintiffs' recovery would no longer be constrained by the ELD nor stymied by tort reforms that deprive plaintiffs of a minimum adequate remedy.

Just as the Magnuson-Moss Consumer Warranty in 1975 was a federal U.C.C. reform addressing misleading U.C.C. warranty titles, disclosures and disclaimers, my proposed federal U.C.C. Article 2 reform proposal would invalidate "no responsibility" clauses that divest the user community of any meaningful remedy for defective software. The immediate impact of this proposed federal reform of Article 2 is that the information industries will no longer be able to use contract law to divest consumers and other licensees of any meaningful remedy for releasing software with vulnerabilities that undermine our private and public infrastructure.

[6] STATE LEGISLATIVE RETRENCHMENT OF PUNITIVE DAMAGES IN 2 PRODUCTS LIABILITY PRACTICE GUIDE § 18.08 ("Hundreds of tort reform statutes were enacted in the 1970s and 1980s. Rustad and Koenig have located 262 tort reform statutes of sixteen basic types that were passed in the fifty states and the District of Columbia. Restrictions on joint and several liability were passed in thirty states. The collateral source rule was passed in twenty-two states. Eighty-five medical malpractice reform statutes were passed in forty-five states. Mandatory structured settlement statutes were passed in twenty states."); Thomas Koenig & Michael Rustad, *His and Her Tort Reform: Gender Injustice in Disguise*, 70 WASH. L. REV. 1, 80–87 (1995) (arguing that women have been disproportionately unable to pursue claims in medical malpractice and products liability actions dues to tort reform).

II. PART I: TODAY'S SOFTWARE CRISIS

A. The Financial Cost of Software Defects

"From damaged database files to generative AI misuse, …high-profile IT disasters wreaked real-world havoc" in 2023.[7] "Both United Airlines and Hawaiian Airlines saw service outages in 2023 resulting from wonky software upgrades, and Southwest ended the previous year with a Christmas travel meltdown blamed on outdated systems."[8] Russia, Iran, North Korea and other adversaries of the United States exploit software vulnerabilities to launch attacks on "financial institutions, against healthcare workers, against education, schools, utilities" to undercut trust in Western institutions.[9] This part of the article documents the cost of widespread software defects, vulnerabilities and anomalies exploited by cybercriminals undermining national security.

Computer scientists use the term, "Software Crisis" to signify "the difficulty of writing useful and efficient computer programs in the required time."[10] Software has become increasingly more complex yet existing methods for designing software have not kept pace. Software engineers explain the software crisis as using the:

> same workforce, same methods, same tools even though rapidly increasing in software demand, the complexity of software, and software challenges. With the increase in the complexity of software, many software problems arise because existing methods were insufficient.[11]

Software anomalies are caused in large part because of the failure of the industry to adequately test and remediate "functional or performance problems disrupting end users' experience."[12] Log4Shell, for example, is a software vulnerability in Apache Log4j 2, a popular Java library which

---

[7] Josh Fruhlinger, *8 Big IT Failures of 2023*, CIO (Dec. 26, 2023), https://www.cio.com/article/1253464/8-big-it-failures-of-2023.html []https://perma.cc/L9FZ-CAJ6].

[8] *Id.*

[9] *How Secure is the U.S. Election System?* WSJ PODCASTS, WALL ST. J. (Jan. 16, 2024) (interviewing Matthew Price, CEO of Cloudfare) (available in LEXIS/NEXIS news file).

[10] *Software Engineering, Software Crisis*, GEEKS FOR GEEKS (Sept. 6, 2023), https://www.geeksforgeeks.org/software-engineering-software-crisis/ [https://perma.cc/7WM4-UE26].

[11] *Id.*

[12] Sandra Felice, *7 Root Causes for Software Defects and How to Overcome Them*, BROWSERSTACK (Dec. 9, 2022), https://www.browserstack.com/guide/root-causes-for-software-defects-and-its-solutions [https://perma.cc/8L63-4SAH].

"enables a remote attacker to take control of a device on the internet if the device is running certain versions of Log4j 2."[13] This Log4Shell or Log4J is the principal instrumentality for cybercriminals to "run virtually any code they want on affected systems, essentially granting them total control of apps and devices."[14]

This tool enables hackers to gain control of computer systems nationwide. "The Log4j vulnerability is "present in major platforms from Amazon Web Services to VMware, and services large and small."[15] The following are the most frequent software vulnerabilities that stem from the industry's failure to implement new methods tailored to increasingly complex software requirements:

• *Errors, oversights or gaps in the original software requirements*. These defects can occur when a requirement is omitted or forgotten, phrased poorly, not properly understood by stakeholders or misunderstood by developers.

• *Errors in the design or architecture of the software*. These problems occur when software designers create an inefficient software algorithm or process, or when that algorithm or process does not yield the required precision in its results.

• *Errors in the coding or implementation*. These defects include traditional bugs caused by everything from missing brackets to ungraceful error handling.

• *Errors in the test planning or test activities*. These defects stem from inadequately tested features and functions.

• *Errors or oversights in the deployment*. An example of these defects would be when a team provisions inadequate VM resources.

---

[13] Andreas Berger, *What is Log4Shell? The Log4j Vulnerability Explained (And What to Do About it)*, DYNATRACE (June 1, 2023), https://www.dynatrace.com/news/blog/what-is-log4shell/ [https://perma.cc/9ZUG-5DC8].

[14] *What is Log4Shell?*, IBM https://www.ibm.com/topics/log4shell#:~:text=Log4Shell%20allows%20hackers%20to%20run%20virtually%20any%20code,granting%20them%20total%20control%20of%20apps%20and%20devices [https://perma.cc/6BLF-ZRDU].

[15] Berger, *supra* note 13.

• *Errors in the process or policies a team uses to govern the development cycle*. These defects crop up when, for example, a team obtains signoffs or approvals without adequate design, coding or testing review.[16]

The principal reasons for the persistence of software errors are: the (1) Lack of Collaboration; (2) Lack of Code Coverage; (3) Poor Test Coverage; (4) Choosing a Wrong Testing Framework; (5) Not Having a Proper Test Reporting System In Place; (6) Lack of a Proper Defect Management Process; and (7) Not Considering Real User Conditions When Testing.[17] The resultant software design issues are partitioned into:

Algorithmic bugs occur because of mistakes in the math or logic used to make the software work.

Logic bugs occur when the software doesn't work properly because of mistakes in writing the code.

Resource bugs occur when the software uses too much memory or other resources, slowing down the computer or causing it to crash.[18]

A software design defect is typically addressed during the testing of computer code, rather than after release in its environment of use.[19] When a software design problem is discovered post-release, and if "a feature does not work as it is supposed to, it is considered a defect."[20] Software defects are further categorized into Integration, Performance, Design, and Logical defects:

Integration defects occur when different software parts do not work together properly.

Performance defects happen when the software does not perform as expected in certain conditions.

---

[16] Stephen J. Bigelow, *How to Handle Root Cause Analysis of Software Defects,* TECHTARGET (Jan. 26, 2021), https://www.techtarget.com/searchsoftwarequality/tip/How-to-handle-root-cause-analysis-of-software-defects [https://perma.cc/F5L3-WAKH].

[17] Felice, *supra* note 12.

[18] Anshuman Singh, *Difference Between Bug and Defect*, SHIKSA ONLINE (June 12, 2023), https://www.shiksha.com/online-courses/articles/difference-between-bug-and-defect/ [https://perma.cc/M4C2-UHJR].

[19] Kalpalatha Devi, *Bug vs. Defect: Core Differences*, BROWSERSTACK (Dec. 16, 2022), https://www.browserstack.com/guide/bug-vs-defect [https://perma.cc/AU9V-VTJB].

[20] Singh, *supra* note 18; Devi, *supra* note 19.

Logical defects are code errors caused by misunderstandings about what the software is supposed to do.

Design defects occur when the software's appearance or functionality is incorrect and can negatively affect a company's reputation.[21]

Poor quality software results in annual expenses and losses which are estimated to be in the range of $2.41 trillion.[22] This approximation includes: cybersecurity failures, including data breaches; operational failures; the cost of finding and fixing defects; unsuccessful development projects; and expenditures in remediating legacy systems.[23] If software specification errors can be detected in the design phase, the design can be modified with relatively little cost.[24] When an error is not detected until it is released into the market, the cost of remediating the defective software to the designer and customer increases significantly.[25]

When software fails, it often results in catastrophic damage. The T-Mobile data breach, for example, resulted in $350 in damages without taking into account customer claims for pay outs."[26] This was the second breach of T-Mobile's computer system of 2022. The first data breach, "which took place in January, affected 37 million customers."[27] A 2022

[21] Singh, *supra* note 18.

[22] "According to the Consortium for Information and Software Quality, poor software quality cost US companies $2.08 trillion in 2020. These losses span all business sectors and include costs from operational failures, unsuccessful projects, and software errors in legacy systems." HERB KRASNER, THE COST OF POOR SOFTWARE QUALITY IN THE U.S.: A 2022 REPORT, *FROM PROBLEM TO SOLUTION*, CONSORTIUM FOR INFORMATION & SOFTWARE QUALITY 3 (Nov. 2022) https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/cpsq-report-nov-22-1.pdf [https://perma.cc/74TQ-5J8V].

[23] *Id.*

[24] *What is the Cost of Defects in Software Testing?* TRYQA, https://tryqa.com/what-is-the-cost-of-defects-in-software-testing/#:~:text=The%20cost%20of%20defects%20can,somewhat%20cheap%20to%20fix%20it [https://perma.cc/5SRH-Z3NQ] (last visited Dec. 8, 2023).

[25] "If however, a defect is introduced in the requirement specification and it is not detected until acceptance testing or even once the system has been implemented then it will be much more expensive to fix. This is because rework will be needed in the specification and design before changes can be made in construction; because one defect in the requirements may well propagate into several places in the design and code; and because all the testing work done-to that point will need to be repeated in order to reach the confidence level in the software that we require." *Id*.

[26] Aaron Drapkin, *Data Breaches That Have Happened in 2022 and 2023 So Far*, TECH.CO (Nov. 6, 2023), https://tech.co/news/data-breaches-updated-list [https://perma.cc/HBR2-N8RF].

[27] *Id.*

ransomware attack misappropriated personal data from customers of three fast food chains: Pizza Hut, KFC, and Taco Bell.[28]

In March 2023, a software defect uncovered that "ChatGPT's open-source library caused the chatbot to leak the personal data of customers, which included some credit card information."[29] Cybercriminals stole 200 million e-mail address from Twitter user selling purloined personal information on the dark web.[30] "Even though the flaw … was fixed in January 2022, the data is still being leaked by various threat actors."[31] In 2013, "a computer glitch nearly pushed investment firm Knight Capital into bankruptcy. The firm lost half a billion dollars in half an hour when a software error allowed computers to buy and sell millions of shares with no human oversight."[32]

The cost of repairing software bugs and defects once the computer code has been released into the marketplace is staggering.[33] It is not just the financial cost of poor software that is concerning, but also the cascading cost of hiring software engineers to detect and fix bugs. "Software companies consume from 50% to 75% of the total budget of software projects in finding and fixing defects in those projects."[34] When a designer releases defective software, the customer must assign database administrators, software engineers, and other technical personnel to detect, remediate, and work around discovered software vulnerabilities.[35]

Remediating bad software "can vary depending on the vulnerabilities' impact and the steps to fix them. Organizations must carefully plan remediation because patches often require downtime or

---

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] Sally Adee, *Bad Bugs: The Worst Disasters Caused by Software Fails*, NEW SCIENTIST (June 5, 2013), https://www.newscientist.com/gallery/software-bugs/ [https://perma.cc/53ZE-7WYP].

[33] "According to the Consortium for Information and Software Quality, poor software quality cost US companies $2.08 trillion in 2020. These losses span all business sectors and include costs from operational failures, unsuccessful projects, and software errors in legacy systems." Laura Marwick, *How Much Could Software Errors be Costing Your Company?*, RAYGUN (July 9, 2023), https://raygun.com/blog/cost-of-software-errors/ [https://perma.cc/Q4RZ-YNGK].

[34] Alia Nabil Mahmoud & Vítor Santos, *Statistical Analysis for Revealing Defects in Software Projects: Systematic Literature Review*, 12 INT'L J. OF ADVANCED COMPUT. SCI. AND APPLICATIONS 237, 237 (2021), https://thesai.org/Downloads/Volume12No11/Paper_28-Statistical_Analysis_for_Revealing_Defects_in_Software_Projects.pdf [https://perma.cc/2EUK-SG89].

[35] *Threat Modeling*, SYNOPSIS, https://www.synopsys.com/glossary/what-is-threat-modeling.html [https://perma.cc/DFM7-4DBC].

have unintended effects."[36] "Usage of third-party components (TPCs) has become the de facto standard in software development."[37] Remediating software defects becomes more challenging because new applications often incorporate third-party libraries, applications, Windows-type interfaces, and distributed applications in their products.

B. Software Vulnerabilities Threaten National Security

Software vulnerabilities not only threaten personal safety, but they also put national security at risk. Defending our nation against cyberattacks is critical to protecting national security as international cybercriminals and "nation-states . . . are developing capabilities to disrupt, destroy, or threaten the delivery of essential services."[38] Cybersecurity and secure software are increasingly synonymous with national security. "China and Russia topped the list of America's online adversaries. But China was deemed the more immediate threat because of the volume of its industrial trade theft."[39] In October 2022, "The National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) exposed the 'Top Common Vulnerabilities and Exposures (CVEs) Actively Exploited by People's Republic of China (PRC) State-Sponsored Cyber Actors' since 2020."[40] In 2024, the FBI warned of the significant risk to

---

[36] *Vulnerability Remediation | A Step-by-Step Guide*, HACKERONE (Sept. 30, 2021), https://www.hackerone.com/vulnerability-remediation-step-step-guide#:~:text=Organizations%20often%20assign%20vulnerability%20disclosures%20to%20staff%20members,vulnerabilities%20while%20development%20teams%20fix%20any%20application%20vulnerabilities [https://perma.cc/N8TP-BLZE]

[37] SAFECODE, MANAGING SECURITY RISKS INHERENT IN THE USE OF THIRD-PARTY COMPONENTS 3 (2017), https://safecode.org/wp-content/uploads/2017/05/SAFECode_TPC_Whitepaper.pdf [https://perma.cc/7QLV-DQ3E] (documenting number of vulnerabilities and security risks in software creating a 'patching frenzy'").

[38] *Cyberthreats and Advisories*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/cyber-threats-and-advisories [https://perma.cc/6YDT-89FG] (last visited Dec. 19, 2023).

[39] Nicole Perlroth, *How China Transformed Into a Prime Cyber Threat to the U.S.*, N.Y. TIMES (July 20, 2021), https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html [https://perma.cc/9SLH-U477].

[40] Press Release, National Security Agency/Central Security Service, NSA, CISA, FBI Reveal Top CVEs Exploited by Chinese State-Sponsored Actors (Oct. 6, 2022), https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3181261/nsa-cisa-fbi-reveal-top-cves-exploited-by-chinese-state-sponsored-actors/ [https://perma.cc/ZL96-UVLV] (stating that "[t]he report highlights how PRC cyber actors continue to exploit these weaknesses to gain unauthorized access into sensitive networks, establish persistence, and move laterally to other internally connected networks. The actors have targeted government and

national security and critical infrastructure posed by economic espionage carried out by Chinese-made drones threatening "critical infrastructure and US national security."[41] "China steals technology from other countries mainly to enhance the economic strength of its companies, and of China itself."[42]

In 2021, hackers originating in The People's Republic of China ("PRC") manipulated vulnerabilities to gain illicit access to several versions of Microsoft ExchangeServer, including "versions that federal agencies hosted and used on their premises."[43] A White House statement revealed that:

> based on a high degree of confidence, malicious cyber actors affiliated with the People's Republic of China's Ministry of State Security conducted operations utilizing these Microsoft Exchange vulnerabilities. The vulnerabilities initially allowed threat actors to make authenticated connections to Microsoft Exchange Servers from unauthorized external sources.[44]

The PRC gained access to Microsoft's ExchangeServer, exploiting software design defects through the following method:

> Once a connection was successfully made, the threat actor could leverage other vulnerabilities to escalate account privileges and install web shells on the affected server. The web shells allowed the threat actor to remotely access a Microsoft Exchange Server, allowing for persistent malicious operations even after the vulnerabilities were patched. According to the advisory, after the initial exploitation of the zero-day vulnerabilities, the threat

---

critical infrastructure networks with an increasing array of new and adaptive techniques—some of which pose a significant risk to Information Technology Sector organizations (including telecommunications providers), Defense Industrial Base (DIB) Sector organizations, and other critical infrastructure organizations.").

[41] Natasha Bertrand, *FBI and CISA Warn Companies to be Wary of Using Chinese-Made Drones over National Security Risks*, CNN WIRE, (Jan. 17, 2024, 4:30 PM), https://www.cnn.com/2024/01/17/politics/fbi-cisa-warning-chinese-made-drones/index.html [https://perma.cc/F7ER-E5Q3].

[42] Hwang Chun-mei, *Taiwan to Change Law to Prevent 'Economic Espionage' by China*, RADIO FREE ASIA (Feb. 2, 2022), https://www.rfa.org/english/news/china/espionage-02172022105135.html [https://perma.cc/FK5N-BEHQ].

[43] *Id.*

[44] U.S. GOVERNMENT ACCOUNTABILITY OFFICE, FEDERAL RESPONSE TO SOLARWINDS AND MICROSOFT EXCHANGE INCIDENTS 16 (2022).

> actors could gain persistent and privileged escalation of accounts to access files and mailboxes on the Microsoft Exchange Server as well as potentially pivot to access other systems and networks within that agency. Further, the persistent access could enable the threat actor to steal credentials and information including PII, encrypt data for ransom, and carry out other types of attacks.[45]

Adversaries can exploit insecure software to learn about troop movements, changes in military missions, and assess readiness. Developing and implementing effective software is essential for learning about the troop movements of adversaries and the likelihood of deployment. National security software needs to be secure and continually updated to address rapidly evolving threats.

The integrity of the U.S. election system also depends upon secure software. In *Curling v. Raffensperger*,[46] the United States District Court for the Northern District of Georgia issued a preliminary injunction order that the state of Georgia had "stood by for far too long" in failing to address the "mounting tide of evidence of the inadequacy and security risks" posed by Georgia's Direct Recording Electronic voting system.[47] The court described Georgia's voting equipment, software, election and voter databases as "antiquated, seriously flawed, and vulnerable to failure, breach, contamination, and attack."[48] The court noted that this was not a hypothetical danger but occurred in:

> 'real life,' this played out with the United States' July 2018 criminal indictment of a host of Russian intelligence agents for conspiracy to hack into the computers of various state and county boards of election and their vendors as well as agents' efforts during the 2016 election to identify election data system vulnerabilities through probing of county election websites in Georgia and two other states.[49]

The continuing vulnerability and unreliability of our voting machines enables unfriendly nation states to interfere with elections that are critically important to upholding democracy. The FBI and other federal

---

[45] *Id*. at 18.
[46] 397 F. Supp. 3d 1334 (N.D. Ga. 2019).
[47] *Id*. at 1338.
[48] *Id.* at 1339.
[49] *Id.* at 1340.

government agencies issued a warning "that threat actors linked to the Russian Foreign Intelligence Service (SVR) are exploiting a critical vulnerability in JetBrains TeamCity software" that could enable supply chain attacks.[50] The Peoples Republic of China ("PRC") has continuously exploited software vulnerabilities in cyberattacks going back to 2014:

> The Microsoft Exchange hack was the latest in a long list of Chinese-sponsored cyberattacks. The tally in just the four years between 2014 and 2018 is head-spinning. There was the Office of Personnel Management attack in which hackers spent some time in OPM networks and then whisked away 21.5 million records from the federal government's background investigation database.[51]

The National Security Agency's ("NSA") cybersecurity advisory calls for preventive measures to address software vulnerabilities exploited by Chinese state-sponsored hackers.[52] The NSA Agency advisory stated that software vulnerabilities are typically "exploited to gain initial access to victim networks using products that are directly accessible from the Internet and act as gateways to internal networks."[53] The NSA proposed the following measures specifically designed to thwart Chinese hackers:

- Keep systems and products updated and patched as soon as possible after patches are released.

- Expect that data stolen or modified (including credentials, accounts, and software) before the device was patched will not be

---

[50] David Jones, *State-Linked Cyber Actors Behind SolarWinds Plant Seeds for New Malicious Campaign*, CYBERSECURITY DIVE (Dec. 15, 2023), https://www.cybersecuritydive.com/news/cyber-actors-solarwinds-new-campaign/702681/ [https://perma.cc/263R-JHTB].

[51] Dina Temple-Raston, *China's Microsoft Hack May Have Had a Bigger Purpose Than Just Spying*, NPR: ALL THINGS CONSIDERED (Aug. 26, 2021, 5:00 AM), https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying [https://perma.cc/P5TT-J69T].

[52] NATIONAL SECURITY AGENCY, CYBERSECURITY ADVISORY, CHINESE STATE-SPONSORED ACTORS EXPLOIT PUBLICLY KNOWN VULNERABILITIES (Oct. 2020), https://media.defense.gov/2020/Oct/20/2002519884/-1/-1/0/CSA_CHINESE_EXPLOIT_VULNERABILITIES_UOO179811.PDF [https://perma.cc/K2WB-5R2R] (documenting how "Common Vulnerabilities and Exposures (CVEs) are exploited by Chinese state-sponsored cyber actors "to enable successful hacking operations against a multitude of victim networks. Most of the vulnerabilities listed below can be exploited to gain initial access to victim networks using products that are directly accessible from the Internet and act as gateways to internal networks.").

[53] *Id.*

alleviated by patching, making password changes and reviews of accounts a good practice.

- Disable external management capabilities and set up an out-of-band management network.

- Block obsolete or unused protocols at the network edge and disable them in device configurations.

- Isolate Internet-facing services in a network Demilitarized Zone (DMZ) to reduce the exposure of the internal network.

- Enable robust logging of Internet-facing services and monitor the logs for signs of compromise.[54]

Chinese hackers misappropriate valuable trade secrets from companies by exploiting known vulnerabilities in popular software applications.[55] Chinese cybercriminals, for example, exploit security vulnerabilities in Microsoft Exchange, Pulse VPN security devices, and other widely deployed applications.[56] In June 2017, the NotPetya malware was released by Russia against the Ukrainian "global transport and logistics giant Maersk, where NotPetya destroyed 'all end-user devices, including 49,000 laptops and print capability,'" and quickly infected computers in sixty countries.[57] "With Ukraine as its primary target, NotPetya quickly spread to more than 60 countries, destroying the computer systems of thousands of multinationals."[58]

NotPetya infected Merck's computer and network system by getting access to [Maersk], a Ukrainian company's computer system, which then developed M.E. Doc, an accounting software used by Merck.[59] The NotPetya malware was transferred in the accounting software, as explained by Merck's experts:

---

[54] *Id.*

[55] Perlroth, *supra* note 39.

[56] *Id.*

[57] "[T]he NotPetya cyber-attack was very likely orchestrated by actors working for or on behalf of the Russian Federation." Merck & Co. v. Ace Am. Ins. Co., 293 A.3d 535, 541 (N.J. Super. 2023); NotPetya: *The Cyberattack That Shook the World*, THE ECON. TIMES: TECH (Mar. 4, 2022), https://economictimes.indiatimes.com/tech/newsletters/ettech-unwrapped/notpetya-the-cyberattack-that-shook-the-world/articleshow/89997076.cms?from=mdr [https://perma.cc/4FCS-BUPL] [hereinafter *NotPetya*: THE ECON. TIMES] (quoting Adam Banks, Maersk Head of Technology).

[58] *NotPetya*: THE ECON. TIMES, *supra* note 57.

[59] *Merck*, 293 A.3d at 539.

> Once on a system or network, NotPetya would attempt to encrypt certain data on the system, rendering the data inaccessible and preventing most users from recovering their files, and once complete, would leave the infected system in an inoperable state. After encrypting data on an infected system or network, NotPetya displayed a message offering to provide a decryption key to recover the data in return for payment of a ransom, presenting itself as ransomware.[60]

The NotPetya malware eventually compromised computers in at least sixty-four different countries.[61]

High profile cyberattacks by Russia and China are targeting federal agencies and U.S. companies, as illustrated by the SolarWinds attack of nine federal agencies in the United States and computer systems in many U.S. companies.[62] Chinese hackers exploited Microsoft Exchange server vulnerabilities infecting "thousands of systems worldwide – as well as a high-profile, though unsuccessful, cyberattack in Florida" on a water treatment facility.[63]

> Software weaknesses are a recognized danger to this nation's critical infrastructure. On January 19, 2023, defective software "result[ed] in almost two hours of grounded flights across the country."[64] Software vulnerabilities have led to catastrophic damages as illustrated by the cancelled flights at Heathrow Airport due to software design problems and Google being forced offline because it was unable to recover from a storage issue. The ransom attack that led Finastra, a leading banking software provider, to take their services offline

---

[60] *Id*. at 540.

[61] *Id.*

[62] Veronica Stracqualursi, *Cyberattack Forces Major US Fuel Pipeline to Shut Down*, WRAL NEWS (May 8, 2021, 10:22 AM), https://www.wral.com/cyberattack-forces-major-us-fuel-pipeline-to-shutdown/19667931/ [https://perma.cc/3GJC-A4J9].

[63] *Id.*

[64] Benefits Ben, *Software Failure at FAA Causes Chaos at Airports*, SERVING THOSE THAT SERVE (Jan. 19, 2023), https://stwserve.com/software-failure-at-faa-2023/ [https://perma.cc/5YDY-Q6RD] ("The software that the FAA states as responsible for the technical failure was installed in 1993 and runs NOTAM (Notice to Air Mission), which provides data that is crucial to pilots successfully navigating the skies. Both the primary and back-up NOTAM software were impacted by a corrupted file.").

> are emblematic of the risk posed by software failure to key industries and infrastructure.[65]

The Federal Bureau of Investigation ("FBI") was able to retrieve "$4.4 million in 'cryptocurrency paid to Colonial Pipeline ransomware attackers.'"[66] The FBI gained "control of DarkSide's proceeds by accessing the private key to the Russian hacker's bitcoin wallet account 'holding about 63.7 bitcoins, worth around $2.3 million.'"[67]

Additionally, in 2019, Russians actors utilized known vulnerabilities in the SolarWinds Orion Software to breach the computer systems of several U.S. federal agencies:

> Then, beginning in February 2020, the threat actor injected malicious code into a file that was later included in SolarWinds Orion software updates. The file was included in several software updates affecting multiple versions of Orion and was available for download from late March to early June, and acted as a Trojan horse, hiding the threat actor's malicious code. SolarWinds released the software updates to its customers not realizing that the updates were compromised with backdoor access from the threat actor. After customers installed the malicious software, the threat actor's malicious file stayed dormant for approximately 2 weeks to avoid detection. Following its dormant period, the threat actor's malicious file activated and began to inspect and gather information on affected systems. Some customers who had downloaded and installed the malicious software updates experienced their systems beaconing out, or connecting, to the threat actor's malicious infrastructure where the threat actor collected the gathered customer information, and determined whether to carry out further command and control activities . . . . [T]he threat actor used the backdoor to send

---

[65] Marwick, *supra* note 33.

[66] Frank Bajak, *$10 Million Rewards Bolster White House Anti-Ransomware Bid*, ASSOCIATED PRESS (July 15, 2021, 9:05 AM), https://apnews.com/article/technology-joe-biden-europe-business-government-and-politics-cd21d84b5fd070421f871610b40e91d0 [https://perma.cc/FF7Z-ZQ94].

[67] Kevin Collier & Pete Williams, *Feds Recover Millions from Pipeline Ransom Hackers, Hint at U.S. Internet Tactic*, NBC NEWS (June 8, 2021, 2:24 PM), https://www.nbcnews.com/tech/security/u-s-recovers-millions-pipeline-ransom-because-hackers-mistake-n1269889 [https://perma.cc/RFZ2-NHTR].

> and install additional malware on customer systems that could be used in post-intrusion activities.[68]
>
> The Pentagon states that the "United States is challenged by malicious cyber actors who seek to exploit our technological vulnerabilities and undermine our military's competitive edge."[69]

State-sponsored Chinese and Russian cybercriminals unleash cyberattacks enabled by defects in software that threaten national security and endanger private companies forced to take their services offside causing untold disruption and consequential damages.

C. Human Loss of Life Caused by Defective Software

Deadly accidents for software defects in medical devices, military equipment, motor vehicles, and airplanes have been attributed to software flaws. Software malfunctions may have latent defects that prove deadly."[70] "Defective software has deadly consequences as illustrated by the following software-related accidents resulting in loss of life or significant economic impact:

- An Iraqi Scud missile hit barracks in Dhahran, Saudi Arabia, after a Patriot missile defense system failed to intercept the missile. The accident resulted in 28 U.S. soldiers killed and 98 soldiers wounded. The failure to intercept the missile was caused by a compounding software clock drift error resulting in a distance calculation error of 687 meters.[71]

---

[68] *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response*, U.S. GOV. ACCOUNTABILITY OFF. (Apr. 22, 2021), https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic [https://perma.cc/SX8E-VHMV].

[69] "The United States is challenged by malicious cyber actors who seek to exploit our technological vulnerabilities and undermine our military's competitive edge," its introduction reads. "They target our critical infrastructure and endanger the American people. Defending against and defeating these cyber threats is a Department of Defense imperative." Colin Demarest, *China, Russia Will Use Cyber to Sow Chaos if War Starts, Pentagon Says*, C4ISRNET (Sept. 12, 2023), https://www.c4isrnet.com/cyber/2023/09/12/china-russia-will-use-cyber-to-sow-chaos-if-war-starts-pentagon-says/ [https://perma.cc/DKL9-KLK5].

[70] Michael L. Rustad, *Torts as Public Wrongs*, 38 PEPP. L. REV. 433, 544 (2011).

[71] Phillip Johnston, *Historical Software Accidents and Errors*, EMBEDDED ARTISTRY (Sept. 20, 2022), https://embeddedartistry.com/fieldatlas/historical-software-accidents-and-errors/ [https://perma.cc/Z6G9-DHPR].

- The Boeing 737 MAX-8 and MAX-9 aircraft were grounded after Ethiopian Airlines and Lion Air crashes both resulted in the deaths of everyone on board. The implicated system is the Maneuvering Characteristics Augmentation System ("MCAS"), which is part of the flight management computer software.[72]

- One of the earliest deadly software cases was the Therac-25 machine which were designed for radiation treatment.[73] "Between 1985 and 1987, in at least six distinct accidents, the Therac-25 radiation therapy machine delivered up to 100 times the prescribed radiation dose, resulting in injury and death."[74] The software for the radiation machine was written by an inexperienced programmer who had limited experience programming for real-time systems. He made few comments and was unlikely to have conducted a timing analysis.[75]

The software errors in the Therac-25 radiation machine led operators to make errors that led to radiation exposures far beyond the prescribed dose:

(1) The operator made an error at the start of the treatment (using the user interface) in the configuration of the machine.

(2) Rectified using the software of the machine.

(3) The user interface indicated that everything was going well or not stopping the process, but it allowed to continue in the operation of the radiation.

---

[72] *Id.*

[73] *Id.*

[74] Michael Barr, *Internationally Recognized Embedded Systems Expert, to Keynote EE Live! 2014 on Embedded Software Safety*, PR NEWSWIRE (Dec. 5, 2013), https://www.prnewswire.com/news-releases/michael-barr-internationally-recognized-embedded-systems-expert-to-keynote-ee-live-2014-on-embedded-software-safety-234622451.html [https://perma.cc/W6A2-XSA4]

[75] Adam Fabio, *Killed by Machine: The Therac-25*, HACKADAY (Oct. 26, 2015), https://hackaday.com/2015/10/26/killed-by-a-machine-the-therac-25/ [https://perma.cc/5HBL-NADN]; *see also* Anne Marie Porrello, *Death and Denial: The Failure of the THERAC-25, A Medical Linear Accelerator*, http://users.csc.calpoly.edu/~jdalbey/SWE/Papers/THERAC25.html [https://perma.cc/VW9P-QDC2] (last visited Dec. 19, 2023) (explaining software errors contributing to Therac-25 disaster).

(4) The patients received radiation up to 125 times higher than what had been configured.[76]

Even as terrifying as the Thera-25 case study is, software defects in linear accelerators continue to harm patients with excessive dosage. The Food and Drug Administration's study of 1,000 radiation therapy cases found most errors were the result of software defects in linear accelerators.[77]

This section has documented that software defects have deadly consequences. No lawsuits have been filed against software makers or engineers that designed code that has failed resulting in death or personal injury.[78] The next section explains how the software industry deploys rights foreclosure clauses to disavow responsibility for buggy or defective software. Immunity breeds irresponsibility such as marketing inadequately tested software. Greater tort liability will lead to better measures to safeguard software..

III. PART II. RIGHTS FORECLOSURE FOR USERS OF DEFECTIVE SOFTWARE

The Biden Administration's Cybersecurity Strategy advises software designers to ramp up cybersecurity so that computer systems cannot be so easily hacked or enable cybercriminals to execute ransomware schemes.[79] The Biden Administration states that this is necessary to realign "incentives to favor long-term investments in security, resilience, and promising new technologies."[80] The Administration's goal is for companies to strengthen software security while preserving the interoperability and openness of the Internet.[81]

\The Introduction to the Cybersecurity Strategy recommends collaboration between "industry; civil society; and State, local, Tribal, and

---

[76] Carlos Caballero, *Software Architecture: Therac-25 the Killer Radiation Machine*, THE STARTUP (May 8, 2019), https://medium.com/swlh/software-architecture-therac-25-the-killer-radiation-machine-8a05e0705d5b [https://perma.cc/U6GM-4YRX].

[77] 1 COMPUTER CONTRACTS § 2.03 (2023).

[78] *Id.*

[79] David E. Sanger, *New Biden Cybersecurity Strategy Assigns Responsibility to Tech Firms*, BOSTON GLOBE (Mar. 2, 2023, 6:19 PM), https://www.bostonglobe.com/2023/03/02/nation/new-biden-cybersecurity-strategy-assigns-responsibility-tech-firms/ [].

[80] NATIONAL CYBERSECURITY STRATEGY, THE WHITE HOUSE, at introduction (Mar. 1, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [https://perma.cc/AF84-WKE6] [hereinafter NATIONAL CYBERSECURITY STRATEGY].

[81] *Id.* at 28.

territorial governments [to] . . . rebalance the responsibility for cybersecurity to be more effective and more equitable."[82] President Biden's strategy highlighted five specific areas: (1) Defend and develop critical infrastructure; (2) Disrupt and dismantle threat actors; (3) Deploymarket forces to drive security and resilence; (4) Invest in a resilent future by safeguarding critical infrastructure; and (5) Enter into international partnerships to pursue shared goals.[83]

Pillar Three of the Administration's Cybersecurity Strategy advocates reallocating "responsibility on those within our digital ecosystem that are best positioned to reduce risk."[84] The objective is greater liability for inadequate software security for data losses and harm caused by inadequate cybersecurity.[85] "Too many vendors ignore best practices for secure development, ship products with insecure default configurations or known vulnerabilities, and integrate third-party software of unvetted or unknown provenance."[86] Pillar Three acknowledges the importance of the marketplace but submits that marketplace solutions alone are insufficient to improve cybersecurity.[87]

An important reason for the continuing epidemic of bad software is that providers use contract law to eliminate all meaningful rights or remedies for the corporate, consumer or organizational user. The current state of U.S. commercial law is that the software industry disavows responsibility for marketing software with known vulnerabilities that enable Chinese cybercriminals and other wrongdoers to endanger national security and misappropriate trade secrets.[88] To date, the software industry

---

[82] *Id.*

[83] Executive Office of the President of the United States, *National Cybersecurity Strategy* (July 31, 2023), Brian Scott, Deputy Assistant National Cyber Director, Cyber Policy & Programs [hereinafter Brian Scott, *National Cybersecurity Strategy*].

[84] NATIONAL CYBERSECURITY STRATEGY, *supra* note 80, at 19.

[85] *Id.*

[86] *Id.* at 20.

[87] *Id.* at 18.

[88] The governments of China, Russia, Iran, North Korea, and other autocratic states exploit software vulnerabilities "with revisionist intent aggressively using advanced cyber capabilities to pursue objectives that run counter to our interests and broadly accepted international norms." Brian Scott, *National Cybersecurity Strategy*, *supra* note 84, at 3. The private or public victims of these cyberattacks have no meaningful cause of action against the software companies enabling these attacks. "The use of disclaimers by the software industry to deny any liability (e.g. for financial or data losses) arising from the customer's use of packaged software has become widespread. Such disclaimers have been recognized in the courts, so long as they are prominently displayed and are explicit." *Question: Software Contracts and Professional Accountability: The Use of Disclaimers by the Software Industry to Deny Any Liability*, CHEGG, https://www.chegg.com/homework-help/questions-and-answers/software-contracts-professional-accountability-use-disclaimers-software-

has not developed an industry standard mandating that software developers or assemblers take prompt remedial action to address software defects that have the potential of causing physical or financial injuries to users.[89]

The Biden Administration calls for placing limits on the ability to shift liability from the software industry to the user.[90] Pillar Three shifts liability back to the software industry by imposing a duty on business organizations to implement reasonable security in their applications and services.[91] By reallocating the cost of software error from the user to the industry, the Biden Administration states that the industry will have the freedom to innovate but must be accountable for excessive, preventable errors.[92] A fence at the top of the cliff is far superior to having an ambulance in the valley below. The Administration acknowledges that too much liability will stifle innovation, especially for small and medium businesses.[93]

This Cybersecurity Strategy pillar requires the Biden Administration to work with Congress, as well as the private sector, to develop legislation and help establish liability-shifting.[94] The Biden Administration contends that by imposing liability on the software industry, which is less costly than imposing on the consumer or other user, by limiting the power of software publishers to shift liability to the user, there is a greater likelihood that publishers will engage in more testing before marketing their

---

industry-deny-liab-q25299049 [https://perma.cc/68CT-H6CE] (last visited Mar. 17, 2024).

[89] Six of the most common software defects include:

(1) Errors, oversights or gaps in the original software requirements. These defects can occur when a requirement is omitted or forgotten, phrased poorly, not properly understood by stakeholders or misunderstood by developers.

(2) Errors in the design or architecture of the software. These problems occur when software designers create an inefficient software algorithm or process, or when that algorithm or process doesn't yield the required precision in its results.

(3) Errors in the coding or implementation. These defects include traditional bugs caused by everything from missing brackets to ungraceful error handling.

(4) Errors in the test planning or test activities. These defects stem from inadequately tested features and functions.

(5) Errors or oversights in the deployment. An example of these defects would be when a team provisions inadequate VM resources.

(6) Errors in the process or policies a team uses to govern the development cycle. These defects crop up when, for example, a team obtains signoffs or approvals without adequate design, coding or testing review.

Bigelow, *supra* note 16.

[90] NATIONAL CYBERSECURITY STRATEGY, *supra* note 80, at 20.

[91] *Id.* at 21.

[92] *Id.*

[93] *Id.* at 20–21.

[94] *Id.* at 21.

applications.[95] The Administration also proposes a Safe Harbor from liability to publishers that "securely develop and maintain their software products and services," acknowledging that secure software development is a moving stream and not a stagnant pond.[96] The Safe Harbor assumes that software design protocol must evolve over time.[97]

The Cyberspace Solarium Commission ("CSC") was established in 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber-attacks of significant consequences."[98] The Cyberspace Solarium Commission's 2020 Report suggests a layered approach to cyber deterrence.[99] The CSC's goal is to

---

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] *Cyberspace Solarium Commission, Introduction*, U.S. CYBERSPACE SOLARIUM COMM'N, https://www.solarium.gov/ [https://perma.cc/U6UD-WW93].

[99] The goal of the layered cyber deterrence approach is to reduce both the probability and deleterious impact of cyberattacks. The Commission's layered approach is predicated upon three means to attain this end:

□ Shape behavior. The United States must work with allies and partners to promote responsible behavior in cyberspace.

The Cyberspace Solarium Report advocates a cybersecurity: layered cyber deterrence whose end objective is to reduce both the probability and the negative impact of cyberattacks should they occur. The Report advocates a new strategic approach to cybersecurity with three deterrent layers to attain the end state:

□ Shape behavior. The United States must work with allies and partners to promote responsible behavior in cyberspace.

□ Deny benefits. The United States must deny benefits to adversaries who have long exploited cyberspace to their advantage, to American disadvantage, and at little cost to themselves. This new approach requires securing critical networks in collaboration with the private sector to promote national resilience and increase the security of the cyber ecosystem.

□ Impose costs. The United States must maintain the capability, capacity, and credibility needed to retaliate against actors who target America in and through cyberspace.

UNITED STATES OF AMERICA: CYBERSPACE SOLARIUM COMMISSION MARCH 2022 REPORT at Executive Summary at 1, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view [https://perma.cc/H2NT-47Q5].

The Commission argues that each deterrent layer will ratchet up both American public- and private-sector security. Six policy pillars implement the three deterrent layers: (1) Reform the U.S. Government's Structure and Organization for Cyberspace; (2) Strengthen Norms and Non-Military Tools; (3) Promote National Resilience. Resilience, the capacity to withstand and quickly recover from attacks that could cause harm or coerce, deter, restrain, or otherwise shape U.S. behavior, is key to denying adversaries the benefits of their operations and reducing confidence in their ability to achieve their strategic ends. (4) Reshape the Cyber Ecosystem. Raising the baseline level of security across the cyber ecosystem—the people, processes, data, and technology that constitute and depend on cyberspace—will constrain and limit

limit the radius of the risk of cyberattacks and the adverse outcomes if one occurred.[100] The Report proposes that Congress enact a statute making the "final goods assemblers of software, hardware, and firmware . . . liable for damages from incidents that exploit known and unpatched vulnerabilities . . . ."[101] The recommendation stemmed from empirical evidence of a widespread pattern of the industry to take prompt remedial action once software vulnerabilities were discovered.[102]

The end goal of software liability is to eliminate liability for defective software through one-sided standard form license agreements that foreclose remedies for marketing insecure software that causes financial injury, property damages, and physical injury. Software makers systematically deploy contract law foreclosure clauses such as complete warranty disclaimers, caps on damages, predispute mandatory arbitration clauses, and anti-class action waivers to disavow responsibility for marketing vulnerable software.[103] President Biden's Cybersecurity Strategy argues that contract law gives providers the means to disclaim liability for failing to address known vulnerabilities and "further reducing

---

adversaries' activities. (5) Operationalize Cybersecurity Collaboration with the Private Sector and (6) Preserve and Employ the Military Instrument of National Power . . . . *Id.*

[100] *Id.*

[101] *Id.* at 76.

[102] Recent empirical studies demonstrate that half of all software design problems and "vulnerabilities remain without a patch for more than 438 days after disclosure that a quarter of vulnerabilities remain without a committed patch beyond three years and there is no correlation between a vulnerability's severity and the length of its lifespan." *Id*.

[103] Apple Computers disclaims all warranties offering their software applications on an "as is" basis. *See e.g.*, Minkler v. Apple, Inc., 65 F. Supp. 3d 810, 819 (N.D. Cal. 2014) ("Here, Apple's Hardware Warranty disclaimed all implied warranties in accordance with California law because it stated in clear language and capitalized formatting that Apple 'disclaims all statutory and implied warranties, including without limitation, warranties of merchantability and fitness for a particular purpose and warranties against hidden or latent defects[,]' [t]he disclaimer is in writing, conspicuous, and mentions merchantability [and] [f]urthermore, Apple's Software Licensing Agreement prominently and conspicuously states that Apple Maps is sold 'as is,' thereby excluding all implied warranties under California law."); *see also* Signal Hound, Inc. v. Expandable Software, Inc., No. C21-5448 BHS, 2022 WL 888353, at *4 (W.D. Wash. Mar. 25, 2022) ("The warranty disclaimer is conspicuous . . . on the first page of a two-page contract, and it includes the heading, 'WARRANTY' in bold and capital letters . . . [t]he provision only contains three sentences after the title, the last of which states [the] . . . warranty is in lieu of all other warranties expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose . . . [and] [t]he fact that the title says 'warranty' and not 'disclaimer of warranty' or something similar does not change the analysis [and] [t]he disclaimer is by no means hidden or difficult to find, and it clearly disclaims the implied warranty of fitness for a particular purpose.").

their incentive to follow secure-by-design principles or perform pre-release testing."[104]

Traditional contract law was "based on consideration, also known as mutuality of obligation."[105] "Courts strive to construe a contract to promote mutuality and to avoid a construction that makes promises illusory."[106] Further, "[t]he modern decisional tendency is against lending the aid of courts to defeat contracts on technical grounds of want of mutuality."[107] The software industry's unilateral discretion in reallocating the risk of injuries or damages from defective software from industry defendants to corporate, organizational, and consumer user communities does not ensure mutuality of obligation. Traditionally, contract law would have invalidated attempts by one party to impose their terms on the other. Software makers and assemblers have created a liability-free zone, a situation which presents an obvious lack of mutuality.

The Biden Administration calls for "shifting the consequences of poor cybersecurity away from the most vulnerable."[108] This part of the article provides strong empirical evidence that software makers, assemblers and other industry defendants systematically eleiminate their responsibility for all warranties and cap damages to a nominal amount. Through disclaimers and limitations of liability, the software industry has effectively shifted the cybersecurity risk to the user.[109] If the 100 largest software companies and the 100 top digital companies deploy contract law to eliminate their legal responsibility for vulnerable software, it is unlikely that the crisis of dangerous defective software can be tackled.

A. Known Vulnerabilities of Microsoft's Software

Microsoft Corporation, founded in 1975, is one of the world's largest technology companies, with revenue of $198 billion in 2022 and market capital of $2 trillion.[110] Microsoft is a pervasive part of everyday life for

---

[104] NATIONAL CYBERSECURITY STRATEGY, *supra* note 80, at 20.

[105] Vice v. E. Texas Mun. Util. Dist., No. 12-21-00225-CV, 2023 WL 3033146, at *4 (Tex. App. Apr. 20, 2023) (quoting Texas Gas Utils. v. Barrett, 460 S.W.2d 409, 412 (Tex. 1970)).

[106] *Id.*

[107] King v. Baylor Univ., 46 F.4th 344, 357 (5th Cir. 2022).

[108] NATIONAL CYBERSECURITY STRATEGY, *supra* note 80, at 19.

[109] John Edward Binkley et al., *Key Takeaways from the National Cybersecurity Strategy*, JD SUPRA (Mar. 8, 2023), https://www.jdsupra.com/legalnews/key-takeaways-from-the-national-4992116/ [https://perma.cc/4VJX-3WYC].

[110] Lionel Sujay Vailshery, *Microsoft—Statistics & Facts*, STATISTA (Sept. 14, 2023), https://www.statista.com/topics/823/microsoft/#topicOverview [https://perma.cc/3NDL-MPFA] (providing Microsoft's revenue during 2022); Jordan Novet, *Microsoft Closes Above $2 Trillion Market Cap for the First Time*, CNBC (June 24, 2021, 4:03 PM), https://www.cnbc.com/2021/06/24/microsoft-closes-

the "1.5 billion active devices running Windows Microsoft Teams."[111] "Microsoft's global PC software market share stood at 83% in 2020. Microsoft is the third-largest seller of smart speakers globally, with a market share of 7% in Q1 2021."[112] Microsoft is ubiquitous in everyday life with its user-friendly tools like Windows, Office and MS Paint.[113]

In 2022, Microsoft reported strong revenue growth for its commercial products: "Its commercial cloud revenue, including Microsoft Azure, Microsoft Office 365 Commercial, and Microsoft Dynamics 365 . . . …increased 32% in FY2022."[114] The Center for Internet Security uncovered multiple vulnerabilities in Microsoft products that could enable remote control execution of the code.

> Two zero-day vulnerabilities addressed in this advisory were reported by Microsoft; both have been seen in the wild. The first zero day, CVE-2023-23397 - Microsoft Outlook Elevation of Privilege Vulnerability, is a privilege elevation bug that allows specially crafted emails to force a target's device to connect to a remote URL and transmit the Windows account's Net-NTLMv2 hash, allowing an attacker to authenticate as the victim. The second zero day, CVE-2023-24880 - Windows SmartScreen Security Feature Bypass Vulnerability, allows an attacker to distribute and install malware by crafting a malicious file that would evade Mark of the Web (MOTW) defenses, resulting in a limited loss of integrity and availability of security features such as Protected View in Microsoft Office, which rely on MOTW tagging.[115]

---

above-2-trillion-market-cap-for-the-first-time.html [https://perma.cc/QR3Z-2RAX] (providing Microsoft's market cap).

[111] Alexander Eser, *Essential Microsoft Statistics in 2024*, ZIPDO (June 9, 2023), https://zipdo.co/statistics/microsoft/ [https://perma.cc/YS3K-ETFQ].

[112] *Id.*

[113] Jason Ward, *How Microsoft's Technological and Social Impacts Have Changed the World*, WINDOWS CENT. (Aug. 12, 2020), https://www.windowscentral.com/microsoft-has-had-profound-technological-and-social-global-impact [https://perma.cc/YCV8-JRK6].

[114] Microsoft Corp; *GlobalData-Swot Analysis* (April. 10, 2023) (available on Lexis' Company and Financial Data).

[115] *Critical Patches Issued for Microsoft Products*, CTR. FOR INTERNET SEC., (Mar. 14, 2023), https://www.cisecurity.org/advisory/critical-patches-issued-for-microsoft-products-march-14-2023_2023-030 [https://perma.cc/PZ93-YRTZ] ("Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged-on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose

In April 2023, Microsoft resolved the following critical vulnerabilities:

- CVE-2023-28285 A Remote code execution vulnerability that affects MS Office allows an attacker to trick users into running malicious files from the local machine to exploit the vulnerability. Also, Microsoft clarifies that it doesn't mean arbitrary code, but the word Remote in the title refers to the attacker's location.

- CVE-2023-28295 & CVE-2023-28287 A Microsoft Publisher remote code execution vulnerability lets hackers gain system access by tricking the users into executing the malicious code that sends via email and downloaded from a malicious website.

- CVE-2023-28311 Microsoft Word Remote Code Execution Vulnerability allows attackers to trick users into running malicious files from the local machine to exploit the vulnerability.[116]

Most "vulnerabilities affecting legacy infrastructure like Microsoft Active Directory continued to burden security teams and present an open door to attackers."[117]

B. Microsoft's Rights Foreclosure Clause

Microsoft's forty-two-page service agreement disavowing responsibility for vulnerabilities in its software applies to the vast majority of its applications and services.[118] Microsoft's user agreement requires all

---

accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.").

[116] Balaji N, *Microsoft Fixed a Windows 0-Day Along With 96 Other Vulnerabilities*, CYBER SEC. NEWS (Apr. 12, 2023), https://cybersecuritynews.com/microsoft-fixed-a-windows-0-day-bug/#:~:text=Microsoft%20Fixed%20A%20Windows%200%2DDay%20Along%20With%2096%20Other%20Vulnerabilities&text=Microsoft%20released%20a%20security%20update,was%20exploited%20for%20ransomware%20attacks [https://perma.cc/RS4E-LJ5X].

[117] CROWDSTRIKE, 2023 GLOBAL THREAT REPORT 2 (2023), https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf [https://perma.cc/2TC6-GJVP].

[118] "The following products, apps and services are covered by the Microsoft Services Agreement, but may not be available in your market[:] Account.microsoft.com, Ask Cortana, Bing Apps, Bing Dictionary, Bing Image and News (iOS), Bing Maps, Bing Pages, Bing Rebates, Bing Search,

users to waive all meaningful rights, warranties, and remedies, while the user may assert his or her rights to the limits of contract law.[119] The first paragraph of Microsoft's standard contract imposes predispute mandatory arbitration to resolve disputes with U.S. users of its products and services.[120]

Consumer arbitration clauses imposed in standard-form contracts are unfair to consumers because they eliminate procedural protections found

---

APIs/SDKs, Bing Search App, Bing Translator, Bing Webmaster, Bing.com, Bingplaces.com, Clipchamp, Collections, Cortana skills by Microsoft, Cortana, Default Homepage, New Tab Page on Microsoft Edge, Dev Center App, Device Health App, Dictate, Education.minecraft.net, Experts for PowerPoint (Preview), Face Swap, Feedback Intake Tool for Azure Maps (aka "Azure Maps Feedback"), Forms.microsoft.com, Forzamotorsport.net, Groove Music Pass, Groove, GroupMe, LineBack, Link to Windows, Maps App, Microsoft 365 Business Standard, Microsoft 365 Business Basic and Microsoft 365 Apps, Microsoft 365 Consumer, Microsoft 365 Family, Microsoft 365 Personal Microsoft Academic, Microsoft account, Microsoft Add-Ins for Skype, Microsoft Bots, Microsoft Collections, Microsoft Defender for individuals, Microsoft Educator Community, Microsoft Family, Microsoft Health, Microsoft Launcher, Microsoft Loop, Microsoft Math Solver, Microsoft Movies & TV, Microsoft Pay, Microsoft Pix, Microsoft Research Interactive Science, Microsoft Research Open Data, Microsoft Search in Bing, Microsoft Soundscape, Microsoft Start, Microsoft Support and Recovery Assistant for Office 365, Microsoft Teams, Microsoft Translator Microsoft Wallpaper, Microsoft XiaoIce, MileIQ, Minecraft games, Minecraft Realms Plus and Minecraft Realms, Mixer, MSN Dial Up, MSN Explorer, MSN Food & Drink, MSN Health & Fitness, MSN Money, MSN News, MSN Premium, MSN Sports, MSN Travel, MSN Weather, MSN.com, Next Lock Screen, Office 365 Pro Plus optional connected experiences, Office for the web (formerly Office Online), Office in Microsoft 365 Consumer, Office in Microsoft 365 Family, Office in Microsoft 365 Personal, Office Store, Office Sway, Office.com, OneDrive.com, OneDrive, OneNote.com, Outlook.com, Paint 3D, Phone Link, Presentation Translator, Rinna, rise4fun, Seeing AI, Send, Skype in the Classroom, Skype Manager, Skype.com, Skype, Smart Search, Snip Insights, Spreadsheet Keyboard, Store, Sway.com, to-do.microsoft.com, Translator for Microsoft Edge, Translator Live, UrWeather, ux.microsoft.com, Video Breakdown, Visio Online, Web Translator, whiteboard.office.com, Windows games, apps and websites published by Microsoft, Windows Movie Maker, Windows Photo Gallery, Windows Store, Windows Live Mail, Windows Live Writer,Word Flow, Xbox Cloud Gaming, Xbox Game Pass, Xbox Game Studios games, apps and websites, Xbox Live Gold, Xbox Live, Xbox Music, Xbox Store, and Zo."

Microsoft Services Agreement, MICROSOFT (July 30, 2023), https://www.microsoft.com/en-us/servicesagreement [https://perma.cc/AW8X-BL2Q].

[119] *Id.*

[120] *Id*. ("Summary of Arbitration Provisions [:] The Microsoft Services Agreement contains binding arbitration and class action waiver terms that apply to U.S. residents. You and we agree to submit disputes to a neutral arbitrator and not to sue in court in front of a judge or jury, except in small claims court.").

in court proceedings, such as the right to an appeal, rules of evidence, constitutional right to a jury, and liberal discovery, which is a right that benefits users disproportionately.[121] A senior attorney for *Public Justice* testified that consumer arbitration clauses "have the effect of immunizing corporations from any liability or accountability even when they have blatantly violated consumer protection or civil rights laws."[122]

Microsoft's asymmetrical clause asserts the unilateral right to change the terms of the agreement and the right to stop offering specific services that it agreed to in its service level agreement upon mere notice to the user.[123] If Microsoft changes its terms, the user's only recourse is to stop using the company's services if the user disagrees with the changed terms.[124] This asymmetrical clause asserts that Microsoft may unilaterally change its user agreement at any time and stop offering services that it agreed to in its service level agreement.[125]

Microsoft's predispute mandatory arbitration clause in its service agreement further couples forced arbitration with a class action waiver.[126] This provision has the legal effect of requiring consumer users to surrender

---

[121] Michael L. Rustad & Thomas H. Koenig, *Empirical Study: Wolves of the World Wide Web: Reforming Social Networks Contracting Practices*, 49 WAKE FOREST L. REV. 1431, 1468 (2014) [hereinafter Rustad & Koenig, *Empirical Study*].

[122] *Id.* at 1468 n.202 (quoting *Arbitration: Is It Fair When Forced*? *Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 60 (2011) (statement of F. Paul Bland, Jr., Senior Attorney, Public Justice) ("In many cases, mandatory arbitration clauses have the effect of immunizing corporations from any liability or accountability even when they have blatantly violated consumer protection or civil rights laws.").

[123] *Microsoft Services Agreement*, *supra* note 118.

[124] *Id.* (Updates to the Services or Software, and Changes to These Terms).

[125] *Id.*

[126] *Id.* ("(15.) Binding Arbitration and Class Action Waiver. If You Live In (or, If a Business, Your Principal Place of Business Is In) the United States. We hope we never have a dispute, but if we do, you and we agree to try for 60 days, upon receipt of a Notice of Dispute, to resolve it informally. If we can't, you and we agree to binding individual arbitration before the American Arbitration Association ("AAA") under the Federal Arbitration Act ("FAA"), and not to sue in court in front of a judge or jury. Instead, a neutral arbitrator will decide and the arbitrator's decision will be final except for a limited right of review under the FAA. Class action lawsuits, class-wide arbitrations, private attorney-general actions, requests for public injunctions, and any other proceeding or request for relief where someone acts in a representative capacity aren't allowed. Nor is combining individual proceedings without the consent of all parties. "We," "our," and "us" includes Microsoft and Microsoft's affiliates.

(a.) Disputes Covered—Everything Except IP. The term "dispute" is as broad as it can be. It includes any claim or controversy between you and us concerning the Services, the software related to the Services, the Services' or software's price, your Microsoft account, advertising, marketing, communications, your purchase transaction, billing, or these Terms, under any legal theory including contract, warranty, tort, statute, or regulation, except disputes relating to the enforcement or validity of your, your licensors,' our, or our licensors' intellectual property rights.").

their right to a jury trial and a judicial reform.[127] In effect, software publishers have constructed a liability-free zone where consumer licensees have rights without remedies if the software provider breaches their license agreement, invades their privacy, or sells their data.[128] The U.S. Supreme Court as well as lower courts have upheld predispute arbitration agreements despite their one-sided nature in consumer transactions.[129]

Microsoft's arbitration clause in its service agreement imposes the American Arbitration Association's ("AAA") Commercial Arbitration rules on all users.[130] The Commercial AAA rules, intended for business

---

[127] *Id.*

[128] 2 COMPUTER CONTRACTS § 8.02 (2023) ("From a licensee's perspective, the use of mandatory arbitration provisions in consumer or employment cases coupled with class action waivers creates, what is in effect, a liability-free zone. The questionable contracting practices of software licensors creates a certainty that consumers enter into these agreements without understanding that they are forfeiting important legal rights. The National Consumer Law Center states that the misuse and abuse of consumer arbitration agreements is the number one consumer problem of the new century. With the U.S. Supreme Court's jurisprudence bringing the full force of the Federal Arbitration Act to bear on consumer arbitrations, it is time for Congress to step in and protect social networking site users from one-sided contracts. There is no question that mandatory arbitration in consumer licensors favors the provider as they can dodge jury verdicts, punitive damages, class actions, consequential damages, and any other meaningful remedy by requiring their users to submit to arbitration. One-sided terms of use that, in effect, divest consumers of fundamental rights raise serious concerns of procedural and substantive unfairness."); *see also* Rustad &. Koenig, Empirical Study, *supra* note 121, at 1455–56; Thomas H. Koenig & Michael L. Rustad, *Fundamentally Unfair: An Empirical Analysis of Social Media Arbitration Clauses*, 65 CASE W. RES. L. REV. 341, 342 (2014); Michael L. Rustad et al., *An Empirical Study of Predispute Mandatory Arbitration Clauses in Social Medial Terms of Service Agreements*, 34 U. ARK. LITTLE ROCK L. REV. 643, 681–82 (2012); Amy J. Schmitz, *Consideration of "Contracting Culture" in Enforcing Arbitration Provisions*, 81 ST. JOHN'S L. REV. 123, 160 (2007) (stating consumers "rarely read or understand" predispute mandatory arbitration agreements).

[129] The U.S. Supreme Court has given lower courts the signal to enforce consumer mandatory arbitration clauses. *See, e.g.*, Marmet Health Care Ctr., Inc. v. Brown, 565 U.S. 530, 532–33 (2012) (striking down West Virginia prohibition against mandatory arbitration clauses in nursing home admissions contracts); Buckeye Check Cashing, Inc. v. Cardegna, 546 U.S. 440, 449 (2006) (holding that "regardless of whether it is filed in federal or state court, a challenge to the validity of a contract as a whole, and not specifically to the arbitration clause" contained within it, must go to the arbitrator and not the court); Green Tree Fin. Corp.-Ala. v. Randolph, 531 U.S. 79, 88–92 (2000) (holding that an order compelling arbitration and dismissing a party's underlying claims is a final decision with respect to arbitration in accordance with FAA § 16(a)(3) and thus immediately appealable; holding that silence in the agreement on the issue of arbitration fees does not render the agreement per se unenforceable for failing to affirmatively protect a party from potentially high arbitration costs).

[130] *Practice Areas*, AM. ARB. ASS'N, https://www.adr.org/commercial [https://perma.cc/YX6C-6XKK]. Microsoft's Service Agreement couples

disputes including large, complex. commercial disputes,[131] is inappropriate for business-to-consumer disputes. The Commercial Arbitration Rules require that the parties deposit the projected cost of the arbitrator's compensation in advance of the arbitration itself.[132] The requirement that consumers have the obligation to pay its share of the arbitrators' compensation alone would preclude them from exercising this remedy as well as filing fees. The filing fee for claims under the $75,000 threshold is $925 and up to $13,750 for the largest claims.[133] In contrast, the AAA's Consumer Arbitration Rules require the consumer to pay $200 and the business is responsible for compensating the arbitrator.[134]

---

commercial arbitration with a prohibition against joining or forming class actions against them. *Microsoft Services Agreement*, *supra* note 118. The AAA's standard commercial arbitration clause has no provision against class actions:

> Any controversy or claim arising out of or relating to this contract, or the breach thereof, shall be settled by arbitration administered by the American Arbitration Association under its Commercial Arbitration Rules, and judgment on the award rendered by the arbitrator(s) may be entered in any court having jurisdiction thereof.

AMERICAN ARBITRATION ASSOCIATION, COMMERCIAL ARBITRATION RULES AND MEDIATION PROCEDURES 8 (2022), https://www.adr.org/sites/default/files/Commercial-Rules_Web.pdf [https://perma.cc/Y2T8-5FXF].

[131] AMERICAN ARBITRATION ASSOCIATION, *supra* note 130, at 9.

[132] *Id.* at 34.

"The AAA will require the parties to deposit in advance of any hearings such sums of money as it deems necessary to cover the expense of the arbitration, including the arbitrator's compensation and expenses, if any, and shall render an accounting to the parties and return any unexpended balance at the conclusion of the case. A party's failure to make the requested deposits by the date established by the AAA may result in the AAA's or the arbitrator's taking any appropriate steps as set forth in Rule R-59.

(b) Other than in cases where the arbitrator serves for a flat fee, deposit amounts requested will be based on estimates provided by the arbitrator. The arbitrator will determine the estimated amount of deposits using the information provided by the parties with respect to the complexity of each case.

(c) The AAA shall request from the arbitrator an itemization or explanation for the arbitrator's request for deposits.

(d) The AAA will allocate the deposits requested among the parties and will establish due dates for the collection of those deposits."

Id. at 34.

[133] AMERICAN ARBITRATION ASSOCIATION, COMMERCIAL ARBITRATION RULES AND PROCEDURES, ADMINISTRATIVE FEE SCHEDULES 1 (2018), https://www.adr.org/sites/default/files/Commercial_Arbitration_Fee_Schedule_1.pdf [https://perma.cc/7ZY6-FW6V].

[134] AMERICAN ARBITRATION ASSOCIATION, CONSUMER ARBITRATION RULES 33 (2016), https://adr.org/sites/default/files/Consumer%20Rules.pdf [https://perma.cc/LG87-4JTB].

Predispute mandatory arbitration clauses deprive users of legal forums ordinarily available to redress claims. The predispute arbitration clause Microsoft deploys also includes, as pro-provider, a choice-of-forum and a choice-of-law provision. When arbitration is imposed, it substitutes the private justice system for the civil justice system.[135]

Microsoft's warranties clause also illustrates a rights foreclosure clause. It is labeled as a warranties clause, when in effect, it is an anti-warranties clause that systematically strips users of any express or implied warranty. Microsoft follows the methodology of U.C.C. § 2-316 in eliminating the implied warranty of merchantability and fitness for a particular purpose when it states it is offering its services on an "as is" or "with all faults" basis.[136] Microsoft also separately disclaims the implied warranty of merchantability and fitness for a particular purpose.[137] Microsoft's warranty disclaimer does not attempt to disclaim express warranties, and the disclaimer makes it clear it is not promising error or interruption of free access.[138]

---

[135] *See* Jessica Silver-Greenberg & Michael Corkery, *In Arbitration, a 'Privatization of the Justice System'*, THE NEW YORK TIMES (Nov. 1, 2015), https://www.nytimes.com/2015/11/02/business/dealbook/in-arbitration-a-privatization-of-the-justice-system.html [https://perma.cc/DQ46-SUH9] ("Over the last 10 years, thousands of businesses across the country— from big corporations to storefront shops—have used arbitration to create an alternate system of justice.").

[136] U.C.C. § 2-316(3). ("(3) Notwithstanding subsection (2)

(a) unless the circumstances indicate otherwise, all implied warranties are excluded by expressions like 'as is', 'with all faults' or other language which in common understanding calls the buyer's attention to the exclusion of warranties and makes plain that there is no implied warranty . . . .").

[137] *Id.* § 2-316(2) ("Subject to subsection (3), to exclude or modify the implied warranty of merchantability or any part of it the language must mention merchantability and in case of a writing must be conspicuous, and to exclude or modify any implied warranty of fitness the exclusion must be by a writing and conspicuous. Language to exclude all implied warranties of fitness is sufficient if it states, for example, that 'There are no warranties which extend beyond the description on the face hereof.'").

[138] *Microsoft Services Agreement*, *supra* note 118.

12. Warranties. MICROSOFT, AND OUR AFFILIATES, RESELLERS, DISTRIBUTORS, AND VENDORS, MAKE NO WARRANTIES, EXPRESS OR IMPLIED, GUARANTEES OR CONDITIONS WITH RESPECT TO YOUR USE OF THE SERVICES. YOU UNDERSTAND THAT USE OF THE SERVICES IS AT YOUR OWN RISK AND THAT WE PROVIDE THE SERVICES ON AN "AS IS" BASIS "WITH ALL FAULTS" AND "AS AVAILABLE." YOU BEAR THE ENTIRE RISK OF USING THE SERVICES. MICROSOFT DOESN'T GUARANTEE THE ACCURACY OR TIMELINESS OF THE SERVICES. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAW, WE EXCLUDE ANY IMPLIED WARRANTIES, INCLUDING FOR MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, WORKMANLIKE EFFORT, AND NON-INFRINGEMENT. YOU MAY HAVE CERTAIN RIGHTS UNDER YOUR LOCAL LAW. NOTHING IN THESE TERMS

Microsoft's warranty clause is another example of a "rights foreclosure" clause. Nowhere in the clause is Microsoft creating warranties. The sole purpose of this clause is to eliminate any warranties of quality, such as the implied warranty of merchantability. Microsoft's warranties clause also disclaims any assurance that its software will work with a particular computer system as it disclaims the warranty of fitness for a particular purpose.[139]

Similarly Microsoft eliminates the warranty of merchantability, which means that it is not willing to represent that its software or operating systems are fit for their ordinary purpose, which is part of the implied warranty of merchantability.[140] The ordinary purpose of software is "to

---

IS INTENDED TO AFFECT THOSE RIGHTS, IF THEY ARE APPLICABLE. YOU ACKNOWLEDGE THAT COMPUTER AND TELECOMMUNICATIONS SYSTEMS ARE NOT FAULT-FREE AND OCCASIONAL PERIODS OF DOWNTIME OCCUR. WE DO NOT GUARANTEE THE SERVICES WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR-FREE OR THAT CONTENT LOSS WON'T OCCUR, NOR DO WE GUARANTEE ANY CONNECTION TO OR TRANSMISSION FROM THE COMPUTER NETWORKS.

Id.

[139] *Id.* Warranty exclusions are permitted under U.C.C. § 2-316. If a warranty disclaimer or limitation is in writing, it must not be in fine print. *See* JAMES J. WHITE ET AL., UNIFORM COMMERCIAL CODE 522 (7th ed. 2022). The disclaimer must be conspicuous to be legally operative. U.C.C. § 2-316(2). Disclaimers are subject to the obligations of good faith and not imposing unconscionable terms upon a party. WHITE ET AL., *supra*, at 518. To exclude or modify the implied warranty of merchantability, the disclaimer must mention merchantability; in the case of a writing, such mention must be "conspicuous." U.C.C. § 2-316(2). A term or clause is conspicuous when it is written so that a reasonable person against whom it is to operate ought to have noticed it. U.C.C. § 1-201(b)(10). The question of conspicuousness is for the court, not the jury. *Id.* The warranties of quality are U.C.C. § 2-313 (express warranty), U.C.C. § 2-314 (implied warranty of merchantability) and U.C.C. §2-315 (fitness for a particular purpose).

[140] *Microsoft Services Agreement*, *supra* note 118. U.C.C. § 2-314 states in relevant part:

(1) Unless excluded or modified (Section 2-316), a warranty that the goods shall be merchantable is implied in a contract for their sale if the seller is a merchant with respect to goods of that kind. Under this section the serving for value of food or drink to be consumed either on the premises or elsewhere is a sale.

(2) Goods to be merchantable must be at least such as

(a) pass without objection in the trade under the contract description; and

(b) in the case of fungible goods, are of fair average quality within the description; and

(c) are fit for the ordinary purposes for which such goods are used; and

(d) run, within the variations permitted by the agreement, of even kind, quality and quantity within each unit and among all units involved; and

(e) are adequately contained, packaged, and labeled as the agreement may require; and

operate computers and execute specific tasks."[141] Microsoft is a trillion-dollar company that disclaims the warranty that its software is fit for its ordinary purpose of executing tasks.[142] Microsoft is unwilling to represent that its software or operating system is at least fair, average, adequately labeled, or that they operate in conformity with representations made in its labeling and packaging.[143]

Not only does Microsoft disclaim all implied warranties, but it also asserts that its warranties clause eliminates express warranties.[144] Any statement that goes to the basis of the bargain is an enforceable express warranty.[145]

Microsoft's description of its products and services creates express warranties if "the seller's description of the good becomes part of the basis of the bargain.[146] Thus, specific statements about the capacity of the seller's computer system represent an enforceable express warranty. For example, the packaging, labeling, and marketing literature for its Windows

---

(f) conform to the promise or affirmations of fact made on the container or label if any.

U.C.C. § 2-314.

[141] Linda Rosencrance, *Software* TECHTARGET: APP ARCHITECTURE (Mar. 2021), https://www.techtarget.com/searchapparchitecture/definition/software [https://perma.cc/Q8VD-NBCP] ("Software is a set of instructions, data or programs used to operate computers and execute specific tasks. It is the opposite of hardware, which describes the physical aspects of a computer. Software is a generic term used to refer to applications, scripts and programs that run on a device. It can be thought of as the variable part of a computer, while hardware is the invariable part.").

[142] Ryan Vlastelica & Dina Bass, *Microsoft Rises to Join Apple in Exclusive $2 Trillion Club*, BLOOMBERG (June 22, 2021, 3:22 PM), https://www.bloomberg.com/news/articles/2021-06-22/microsoft-rallies-to-join-apple-in-exclusive-2-trillion-club#xj4y7vzkg [https://perma.cc/JP8D-LWLV] ("Microsoft Corp. took its place in the history books as just the second U.S. public company to reach a $2 trillion market value, buoyed by bets its dominance in cloud computing and enterprise software will expand further in a post-coronavirus world.").

[143] *Microsoft Services Agreement*, *supra* note 118 (making no warranties, express or implied); U.C.C. § 2-314(2) (stating that for goods to be merchantable they must be of "fair average quality within the description," "adequately contained, packaged, and labeled as the agreement may require," and "conform to the promises or affirmations of fact made on the container or label").

[144] *Microsoft Services Agreement*, *supra* note 118 (making no warranties, express or implied).

[145] U.C.C. § 2-313(1); Henry v. Campbell Soup Co., No. 22-CV-431 (LDH) (PK), 2023 WL 2734778, at *22 (E.D.N.Y. Mar. 31, 2023) ("In New York, '[a]ny description of the goods which is made part of the basis of the bargain creates an express warranty that the goods shall conform to the description.'") (quoting N.Y. U.C.C. § 2-313(1)(b)).

[146] WHITE ET AL., *supra* note 140, at 409 ("Descriptions are a particularly important subset of factual affirmations. ("It is not uncommon for a court to label an express warranty both descriptions under 2-313(1)(b) and an affirmation of fact under 2-313(1)(a)").

software will make statements constituting express warranties.[147] Microsoft states in its advertisement for Microsoft 365 Family and Microsoft 365 Personal that:

> Ransomware detection notifies you when your OneDrive files have been attacked and guides you through the process of restoring your files. Ransomware is a type of malicious software (malware) designed to block access to your files until you pay money. When Microsoft 365 detects a ransomware attack, you will be notified on your device and receive an email from Microsoft 365 . . . . If Microsoft 365 detected a ransomware attack, you see the Signs of ransomware detected screen when you go to the OneDrive website.[148]

Microsoft's statements implying that its products have ransomware protection and a means to recover files from malicious attacks are "affirmations of fact" sufficiently specific to constitute an enforceable express warranty, rather than puffery or seller's talk.[149] If a Microsoft user does not receive a notification or e-mail after a ransomware attack, the user would have an express warranty cause of action.

Microsoft also makes express warranties when it describes its many products and services on its website.[150] Statements made that apply to the

---

[147] *Microsoft – Terms of Use*, MICROSOFT (Feb. 7, 2022), https://www.microsoft.com/en-us/legal/terms-of-use [https://perma.cc/YC7F-46MH]. "Any affirmation of fact or promise made by the seller to the buyer which relates to the goods and becomes part of the basis of the bargain creates an express warranty that the goods shall conform to the affirmation or promise." TENN. CODE § 47-2-313(1)(a). In addition, "[a]ny description of the goods which is made a part of the basis of the bargain creates a warranty that the goods shall conform to the description." *Id.* § 47-2-313(1)(b). No specific words are necessary to create an express warranty; rather, express warranties are "dependent on the party's intention." Brown v. Woodbury Auto Grp. LLC, No. 3:21-cv-00955, 2023 WL 2529055, at *11–12 (M.D. Tenn. Feb. 22, 2023) (quoting Coffey v. Dowley Mfg., Inc., 187 F. Supp. 2d 958, 970 (M.D. Tenn. 2002)).

[148] *Ransomware Detection and Recovering Your Files*, MICROSOFT, https://support.microsoft.com/en-us/office/ransomware-detection-and-recovering-your-files-0d90ec50-6bfd-40f4-acc7-b8c12c73637f [https://perma.cc/AN7U-N43M] (last visited Dec. 21, 2023).

[149] *Id.*; WHITE ET AL., *supra* note 139, at 401, 410 (explaining factors separating express warranties from statements of opinion or seller's talk).

[150] *See, e.g.*, *Surface Laptop 5*, MICROSOFT, https://www.microsoft.com/en-us/d/surface-laptop-5/8xn49v61s1bn?activetab=pivot:fulltechspecstab [https://perma.cc/8AWX-KMTX] (last visited Dec. 21, 2023); *see also* Presnell v. Snap-On Securecorp, Inc., 583 F. Supp. 3d 702, 710 (M.D.N.C. 2022) ("It is well-settled that language on a defendant's website can constitute an express warranty.").

basis of the bargain are nondisclaimable.[151] Many computer contracts *attempt* to disclaim express warranties, but the only way to truly avoid liability for express warranties is self-restraint. The express warranty is as "tenacious as a bulldog, and the only way to get rid of it is to see that it never takes hold."[152] The disavowal of express warranties is "disfavor[ed]."[153] Microsoft is precluded from stating that its user has ransomware protection and then later disavowing that representation in its Warranties Clause.[154]

Microsoft imposes a cap on damages of either what the user paid for the month during which the loss or damages occurred or $10.00.[155] His cap on damages is a rights foreclosure because it makes it cost prohibitive to file a claim against Microsoft when it breaches its service agreement. The limitation of the liability clause caps Microsoft's total damages to a nominal amount of $10 when it states:

> 13. Limitation of Liability. If you have any basis for recovering damages (including breach of these Terms), you agree that your exclusive remedy is to recover, from Microsoft or any affiliates, resellers, distributors, Third-Party Apps and Services providers, and vendors, direct damages up to an amount equal to your Services fee for the month during which the loss or breach occurred (or up to $10.00 if the Services are free). You can't recover any other damages or losses, including direct, consequential, lost profits, special, indirect, incidental, or punitive. These limitations and exclusions apply even if this remedy doesn't fully compensate you for any losses or fails of its essential purpose or if we knew or should have known about the possibility of the damages. To the maximum extent permitted by law, these limitations and exclusions, apply to anything or any claims related to these Terms, the Services, or the software related to the Services.[156]

---

[151] WHITE ET AL., *supra* note 139, at 505 ("To begin, a 'disclaimer' of an express warranty may seem an oxymoron. How can a seller disavow an express representation that by hypothesis and definition is 'part of the basis of the bargain?'").

[152] THOMAS M. QUINN & LOUIS F. DEL DUCA, UNIFORM COMMERCIAL CODE COMMENTARY AND LAW DIGEST 182 (1st ed. 1978).

[153] WHITE ET AL., *supra* note 139, at 505 ("As finally adopted, however, section 2-316(1) is not quite so stark, but it clearly disfavors the disavowal of express warranties.").

[154] *Id.*

[155] *Microsoft Services Agreement*, *supra* note 118.

[156] *Id.* (emphasis in the original).

The next section will determine whether "no responsibility clauses (otherwise known as "rights foreclosure clauses") found in Microsoft's standard form agreements) reflect a general trend in the software industry. Microsoft's use of foreclosure clauses reflects a larger trend in the software industry of offering its standard products without warranties nor meaningful remedies.

C. Clauses Employed By the One Hundred Top Software Companies

1. Prior Empirical Studies of Software Licensing

There is almost no empirical research on the use of "no responsibility" clauses such as disclaimers and caps on damages to a nominal amount by the software or digital services industry. A notable exception is a New York University ("NYU") study which examined how provisions of consumer agreements changed from 2003 and 2010.[157] The NYU study examined changing terms of 264 mass-market consumer software license agreements.[158] The overall finding was that software and digital industry companies implemented many changes in their license agreements over the seven-year period of the study.[159] The NYU researchers documented that nearly four in ten of the sample firms studied made material changes to their standard form contracts.[160]

The NYU researchers found that "[c]ontracts have also gotten considerably longer on average but no easier to read; despite being ostensibly written for the consumer, the average license agreement remains, by standard textual analysis criteria, as hard to read as an article in a scientific journal."[161] The NYU research team also found "that most of the terms that changed have become more pro-seller relative to the

---

[157] Florencia Marotta-Wurgler & Robert B. Taylor, *Set in Stone? Change and Innovation in Consumer Standard-Form Contracts*, 88 N.Y.U. L. REV. 240, 243 (2013).

[158] *See id.* We use a sample of EULAs from 264 mass-market software firms between 2003 and 2010 to track changes to thirty-two common contractual terms. Our methodology measures the relative buyer-friendliness of each term relative to the default rules of Article 2 of the Uniform Commercial Code (U.C.C.) to examine how the pro-seller bias of EULAs changes over time. Since buyers need to become informed about terms to "shop" around effectively, we measure changes in contract length and readability. We begin exploring the firm, product, and market characteristics that are associated with contract changes. Finally, we record relevant court decisions around the sample period to evaluate whether the sample contracts are sensitive to changes in the enforceability of terms. *Id.*

[159] *Id.* at 274–75.

[160] *Id.* at 243–44.

[161] *Id.* at 244.

original contract. Most of these changes are driven by firms opting out of U.C.C. Article 2 default rules in favor of relatively more pro-seller terms."[162]

This next section is my study of the incidence and use of rights foreclosure, also known as "rights foreclosure" clauses in the 100 largest digital companies in the world. The overwhelming conclusion of my empirical study is that the largest software companies in the world offer their applications and operating systems without giving consumers a meaningful, minimum remedy when they breach their license and service agreements.

2. Description of the Sample of the 100 Largest Software Companies

The sample of software industry companies is drawn from The Software Report's list of "The Top 100 Software Companies of 2021."[163] The list of top 100 software companies included a wide range of well-

---

[162] *Id.*

[163] *The Top 100 Software Companies of 2021*, THE SOFTWARE REP. (July 12, 2021), https://www.thesoftwarereport.com/the-top-100-software-companies-of-2021/ [https://perma.cc/SW9J-2T9G] [hereinafter *Top 100 Software*] (The one hundred top software companies ranked 1 to 100 are: (1) Microsoft (USA), (2) Adobe (USA), (3) ServiceNow (USA) (4) Dropbox (USA), (5) IFS (Sweden), (6) Guidewire (USA), (7) Cornerstone USA), (8) Secureworks (USA), (9) Vertafore (USA), (10) Procore (USA), (11) Asana (USA), (12) ICIMS (USA), (13) Autodesk (USA), (14) Intuit (USA), (15) Altimetrik (USA), (16) Workday (USA), (17) Salesforce, (18) the Trade Desk (USA), (19) Qualtrics (USA), (20) Blackline (USA), (21) Cisco Systems (USA), 22 Nintex (USA), (23) PowerSchool, (24) Twillo (USA), (25) Gainsight (USA), (26) Zoho (India), (27) Atlassian (Australia), (28) Vmware (USA), (29) Shopify (Canada) (30) Cvent (USA), (31) Talend (USA), (32) Templafy (Denmark), (33) Cloudfare (USA), (34) MURAL (USA), (35) Stack Overflow (USA), (36) DataRobot (USA), (37) Acquiva (USA), (38) Imply (USA), (39) Argo AI (USA), (40) Hootsuite (Canada), (41) Samdsara (USA), (42) Planview (USA), (43) airSlate (USA), (44) Iterable (USA), (45) Sisense (USA), (46) Pipedrive (USA), (47) Pax8 (USA), (48) Outreach (USA), (49) Fivetran (USA), (50) Absolute Software (Canada), (51) Mapbox (USA), (52) Code42 (USA), (53) Sendinblue (France), (54) Alida (Canada) (55) FiscalNote (USA), (56) StellarWP (57) QGenda (USA), (58) Articulate (USA), (59) Pantheon (USA), (60) Namely (USA), (61) Conductor (USA), (62) Grammarly (USA), (63) UserZoom (USA), (64) Kibo (USA), (65) Panopto (USA), (66) Notarize (USA), (67) Botkeeper (USA), (68) JungleScout (USA), (69) Lever (USA), (70) Influitive (Canada), (71) Simpplr (USA), (72) vcita (Israel), (73) Visual Lease (USA), (74) Widen (USA), (75) WhereScape (USA), (76) General Global Assistance (USA), (77) Dealer Socket (USA), (78) Domo (USA), (79) Genesys (USA), (80) Intapp (USA), (81) ASAPP (USA), (82) Broadridge Financial Services (USA), (83) Fastly (USA), (84) Ascent (United Kingdom (85) Verkada (USA), (86) CloudPay (United Kingdom), (87) FourKites (USA), (88) Gofore (Finland), (89) Identiv (USA), (90) Murex (France), (91) mParticle (USA), (92) League (Canada), (93) Protgrity (USA), (94) iBoss (USA), (95) Fireflies.ai (USA), (96) Bringg (Israel), (97) Heap (USA), (98) Aclima (USA), (99) Drift (USA), and (100) Beamery (United Kingdom)).

known companies such as Microsoft, Adobe, Dropbox and Salesforce, but also less known companies such as IFS, Guidewire, Cornerstone, Procore, and Asana.[164] Of the top ten companies, nine of them were headquartered in the U.S., while Sweden's IFS was the only non-U.S. company. The top ten largest software companies are depicted in Chart Two below.

Chart Two: Top Ten Software Companies of 2021

Company Name	*Typical Products*	*Examples of Software Vulnerabilities*
(1) Microsoft (USA), (2 trillion valuation in June 2021[165])	Microsoft Office Suite, Internet Explorer, Edge Web Browser, LinkedIn, Xbox	Between 2014 and early 2024, CVE Detail uncovered 11,351 vulnerabilities in Microsoft products.[166] Between 2014 and 2024, CVE Detail found 3,057 vulnerabilities

[164] *Id.* As documented in Chart Two, the top ten software companies tend to be classified as companies that create software applications. *Id.* Microsoft, for example, produces its Office Suite, search engine, web browser, and social media site. *Id.* Adobe, for example produces traditional software applications as well as cloud and subscription-based products. *Id.*; *see also supra* Chart Two. Forbes list of the top 100 digital companies shows that digital companies have more diverse products including electronics, broadcasting and cable, Internet catalogues, semiconductors, and business and personal services. *Top 100 Digital Companies*, FORBES (2019), https://www.forbes.com/top-digital-companies/list/#tab:rank [https://perma.cc/A973-KCGN] [hereinafter *Top 100 Digital*]. There is some overlap between the list of the 100 largest software companies and the 100 top digital companies. *See id.*; *see also Top 100 Software*, *supra* note 163. For example, Apple and Microsoft are listed on both top 100 lists. *See Top 100 Digital*, *supra*; *see also Top 100 Software*, *supra* note 163. The conclusion is that the 100 largest digital companies represent more diverse industries than the top 100 software companies. *See Top 100 Digital*, *supra*; *see also Top 100 Software*, *supra* note 163. Neither the top 100 digital company or software lists defines what they mean by digital company or software company. *See Top 100 Digital*, *supra*; *see also Top 100 Software*, *supra* note 163. Including both groups in my empirical study provides strong unobtrusive evidence that the largest and most powerful companies in the world are deploying rights foreclosure or no responsibility clauses such as warranty disclaimers, caps on damages, mandatory arbitration clauses coupled with anti-class action waivers and other one-sided clauses that deprive consumer of any meaningful remedy.

[165] *Top 100 Software*, *supra* note 163.

[166] *Microsoft: Security Vulnerabilities, CVEs*, CVE DETAILS, https://www.cvedetails.com/vulnerability-list/vendor_id-26/Microsoft.html [https://perma.cc/G5S3-XXCS] (number of vulnerabilities updated as of March 17, 2024).

		impacting Code Execution, 73 vulnerabilities enabling Bypass, 2,182 allowing Privilege Escalation, 1,037 Denial of Service, and 1,229 vulnerabilities allowing information leak. [167] Microsoft's products have known exploited vulnerabilities.[168]
(2) Adobe (USA) (quarterly revenue of $3.91 billion in Q1 2021.[169]	Traditional Software Packages, Cloud, and Subscription-Based Products	A total of 10, 870 vulnerabilities were uncovered in 194 Google products including well-known products such as Google AdSense, Google Analytics. Google Authenticator, Google Doc Embedder, Google Forms, and Google Maps.[170] 'The Adobe patches include one for a vulnerability in the Adobe Download Manager for Windows that allows an attacker to escalate privileges within the system, potentially letting a hacker compromise the processing resources of a user's computer. Eran

[167] *Microsoft Vulnerability Statistics* (2014-2024), *Vulnerabilities by Impact Types*, CVE DETAILS, https://www.cvedetails.com/vendor/26/Microsoft.html [https://perma.cc/X9WZ-26QP] (last visited Jan. 2024).

[168] *See e.g.*, *Microsoft SharePoint Server Elevation of Privilege Vulnerability*, *CVE-2023-29357, Known Exploited Vulnerability*, CBE DETAILS, https://www.cvedetails.com/cisa-known-exploited-vulnerabilities/kev-1.html [https://perma.cc/52YJ-65PY].

[169] *Top 100 Software*, *supra* note 163.

[170] *Vendor Search: Google*, CVE DETAILS, https://www.cvedetails.com/vendor-search.php?search=google [https://perma.cc/DA6D-4295] (last visited Jan. 2024).

		Shimony of CyberArk first discovered the vulnerability, marked CVE-2019-8071, and a patch is now available. In the update APSB19-49 Adobe has identified 68 security total issues relating to Adobe Acrobat and Reader.'[171] In 2023, Adobe "fixed vulnerabilities that could affect specific versions of Adobe products."[172] CVE detail documented that cybercriminals exploited a known vulnerability in Adobe ColdFusion: "Adobe ColdFusion versions 2018u17 (and earlier), 2021u7 (and earlier) and 2023u1 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution."[173]
(3) ServiceNow (USA), ($108 billion	Software as a Service, Work Flow Software	CVE Detail reported eight vulnerabilities in

[171] *Adobe Patches 45 Critical Vulnerabilities, Including a Download Manager Vulnerability*, TECHMONITOR (Oct 16, 2019), https://techmonitor.ai/hardware/adobe-patches-adobe-download-manager [https://perma.cc/9K3L-783E] ("Adobe has identified 68 security total issues relating to Adobe Acrobat and Reader.... Adobe is warning that these critical and important vulnerabilities could lead to hackers successfully carrying out an arbitrary code execution which has the same level of security clearance as the user. The San Jose creative software firm has rolled out the APSB19-49 update to address all 68 issues and is advising users and IT teams to either manually update or initiate the update via the enterprise installer.").

[172] Balaji N, *supra* note 116.

[173] *Security Vulnerabilities, CVEs, in CISA KEV Catalog*, CVE DETAIL, https://www.cvedetails.com/cisa-known-exploited-vulnerabilities/kev-1.html [https://perma.cc/W5EB-LRY4].

market capitalization)[174]		ServiceNow Software between 2014 and 2024.[175] For example, a "cross-site scripting (XSS) vulnerability in Employee Service Center (esc) and Service Portal (sp) in ServiceNow Quebec, Rome, and San Diego allows remote attackers to inject arbitrary web script via the Standard Ticket Conversations widget."[176] CISA reported, "Adobe has released security updates to address multiple vulnerabilities in Adobe software. An attacker can exploit these vulnerabilities to take control of an affected system."[177]
(4) Dropbox (USA) ($2 billion annual revenues)	Cloud Storage & Management	Dropbox is one of the most popular cloud storage solutions in the world, supporting more than 14 million paying customers… The most infamous Dropbox data breach "included the theft of more than 68 million account

[174] *Top 100 Software*, *supra* note 163 (describing the #3 ranked software company).

[175] *ServiceNow Vulnerabilities*, CVE DETAILS, https://www.cvedetails.com/product-search.php?vendor_id=0&search=ServiceNow [https://perma.cc/5NRC-XHFH] (results of Product Search) (as of Jan. 2024).

[176] *Security Vulnerabilities*, CVE DETAILS, https://www.cvedetails.com/vulnerability-list/vendor_id-17782/Servicenow.html [https://perma.cc/JBD7-WJVK] (last visited Dec. 21, 2023).

[177] *Known Exploited Vulnerabilities Catalog*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/known-exploited-vulnerabilities-catalog [https://perma.cc/P6FN-TCR9] (last visited Dec. 21, 2023).

		credentials in 2012 (hackers tried to sell this data in 2016), and the hack led to the company resetting passwords for millions of accounts in 2016."[178] CVE Detail described the following Dropbox vulnerability trends from 2017 to 2022: Overflow (3 vulnerabilities), Memory Corruption (2 vulnerabilities), and Input Validation (1 vulnerabilities).[179] CVE Detail also examine Dropbox vulnerabilities by impact: Bypass (3), Privilege Escalation (3), Denial of Service (5), and Information Leak (1).[180]
(5) IFS (Sweden)[181] ("FY2022 IFS software revenue was 6.6 billion Swedish Krona (SEK), which is about $634.8 million USD, up 28 percent YoY from 2021. FY2022 IFS	Enterprise Software, Software for aerospace and defense, energy, manufacturing engineering and services.	"IFS Developer Studio update…This update contains the fix (JndiLookup.class removal) that mitigates the log4j vulnerability CVE-2021-44228 when deploying to the local server on the

[178] Dave Johnson, *Is Dropbox Secure? Here's How Dropbox Has Improved its Security Measures, and What You Can do to Protect Yourself*, BUS. INSIDER (Mar. 4, 2021, 3:19 PM), https://www.businessinsider.com/guides/tech/is-dropbox-secure [https://perma.cc/ZHQ3-RWRL].

[179] *Dropbox: Vulnerability Statistics*, CVE DETAILS, https://www.cvedetails.com/vendor/11159/Dropbox.html [https://perma.cc/L8YB-BZ3X] (last visited Jan. 2024).

[180] *Id.*

[181] *Top 100 Software*, *supra* note 163 (describing the #5 ranked software company).

overall recurring revenue 6.1 billion SEK, which is about $586.6 million USD, an increase of 44 percent YoY from 2021."[182]		developer machine. Please read the KBA article for information on how the tool is updated."[183]
(6) Guidewire Software (USA)[184] ("Total revenue for fiscal year 2020 was 742.3 million; As of April 30, 2021, revenue was up from $514 million on July 31, 2020.").[185]	"Guidewire combines digital, core, analytics and AI to deliver its platform as a cloud service."[186]	"Ethos Technologies Inc. and Guidewire Software Inc. have been hit with a class action lawsuit alleging they failed to adequately safeguard sensitive data, leaving the information vulnerable to a targeted cyberattack."[187]
(7) Cornerstone (USA)[188] ("Cornerstone had a strong start to 2021	Makers of comprehensive recruiting software, which it licenses to 6,000 organizations "spanning more than	"SQL injection vulnerability in default.php in Cornerstone Technologies webConductor allows

[182] *IFS Performance Outpaces Competitors With 5th Consecutive Year of Double-Digit Growth*, IFS NEWSROOM (Jan. 23, 2023), https://www.ifs.com/news/earnings/ifs-performance-outpaces-competitors-with-5th-consecutive-year-of-double-digit-growth [https://perma.cc/CLQ6-ZETU].

[183] *Urgent Bulletin - IFS Advisory: IFS Products, Services and Log4j - CVE-2021-44228*, IFS, https://community.ifs.com/announcements-278/urgent-bulletin-ifs-advisory-ifs-products-services-and-log4j-cve-2021-44228-16436 [https://perma.cc/EY7S-QK5C].

[184] *Top 100 Software*, *supra* note 163 (describing the #6 ranked software company).

[185] *Id.*

[186] *Id.*

[187] Anne Bucher, *Guidewire Class Action Claims Recent Data Breach Compromised Consumer Information*, TOP CLASS ACTIONS (Jan. 5, 2023), https://topclassactions.com/lawsuit-settlements/privacy/data-breach/ethos-guidewire-class-action-claims-recent-data-breach-compromised-consumer-information/ [https://perma.cc/X65K-FXLD] (describing Christopher Stein's class action lawsuit in California federal district court against Ethos Technologies Inc. and Guidewire Software Inc. for "allegedly failing to safeguard sensitive data, leaving it vulnerable to a targeted cyberattack from August through December 2022.").

[188] *Top 100 Software*, *supra* note 163 (describing the #7 ranked software company).

with Q1 revenue of $209.3 million."[189]	75 million users across over 180 countries."[190]	remote attackers to execute arbitrary SQL commands via the id parameter."[191]
(8) SecureWorks (USA) (global cybersecurity and cloud security analytics).[192]	Global cybersecurity, cloud security analytics platform, cloud SaaS solutions to respond to attacks [193]	N/A, SecureWorks specialty is "audits across internal and external network devices, servers, web applications, databases, and other assets in your on-premises and cloud environments."[194] CVE Detail uncovered no vulnerabilities for all versions of Dell's SecureWorks.[195]
(9) Vertafore (USA) (simplify and automate insurance distribution).[196]	InsurTech company with software solutions to automate end-to-end processes.[197]	None
(10) Procore (USA)[198] (construction	Construction Management Software for owners,	None

[189] *Id.*

[190] *Id.*

[191] *Vulnerability Summary for the Week of January 28, 2013*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Feb. 4, 2013), https://www.cisa.gov/news-events/bulletins/sb13-035 [https://perma.cc/UZZ5-NPMX] (High Vulnerabilities, 2013-01-31, "CVE-2010-5287 SQL injection vulnerability in default.php in Cornerstone Technologies webConductor allows remote attackers to execute arbitrary SQL commands via the id parameter.").

[192] *Top 100 Software*, *supra* note 163 (describing #8 ranked software company)

[193] *Id.*

[194] *Data Sheet: Managed Vulnerability Scanning: Identify Vulnerabilities and Reduce Risk*, SECUREWORKS, https://www.secureworks.com/resources/ds-managed-vulnerability-scanning[https://perma.cc/B8MC-SJMK] (last visited Dec. 21, 2023) (describing business model of scanning clients' websites, products, databases, and other assets for software vulnerabilities).

[195] *Dell Secureworks: Product Details, Threats and Statistics*, CVE DETAILS, https://www.cvedetails.com/product/33410/Dell-Secureworks.html?vendor_id=2234 [https://perma.cc/T39K-FHU2] (last visited Jan. 2024).

[196] *Top 100 Software*, *supra* note 163 (describing #9 ranked software company).

[197] *Id.*

[198] *Id.* (describing #10 ranked software company).

management software licensor)	general contractors, and specialty contractors. "Procore is the only real software platform in the construction industry that creates a central collaboration hub for owners, general contractors, specialty contractors, and other project collaborators across the entire project lifecycle."[199]	

As Chart Two reveals, seven of ten of the largest software companies in the world have released software into the marketplace with numerous known vulnerabilities. The three exceptions were Vericore, whose software automates the distribution of insurance, and Procore, which markets construction software and Dell SecureWorks, a leading Managed Service Provider.[200] Vulnerabilities were assessed from an analysis of Cybersecurity & Infrastructure Agency's Known Exploited Vulnerabilities Catalogue.[201] The overwhelming conclusion is that the largest software companies have known vulnerabilities in their software that can be exploited by cybercriminals.

3. Rights Foreclosure Clauses in the Software Industries

Software vendors generally draft clauses that take away rights and remedies at a reading level far beyond the reading comprehension of an average American consumer. The standard form agreements were drafted at a reading level only understood by users with two or more years of college education (Grade 14).[202] At best, the standard form agreements

---

[199] *What is Procure?*, PROCORE, https://www.procore.com/what-is-procore [https://perma.cc/VD4Y-WDLW] (last visited Dec. 21, 2023).

[200] *The Dell SecureWorks Difference*, DELL SECUREWORKS, https://i.dell.com/sites/csdocuments/Shared-Content_data-Sheets_Documents/en/secureworks-difference.pdf [https://perma.cc/E6CE-9GJY] (at 2) ("Monitoring thousands of customers in more than 70 countries provides Dell SecureWorks with unique visibility into the evolving threat landscape.").

[201] *Known Exploited Vulnerabilities Catalog*, *supra* note 177.

[202] The software license agreements as a whole were tested for readability as well as compared to warranty disclaimers, limitation of liability, arbitration/anti-class action waivers, and other rights foreclosure or "no responsibility" clauses using the

deployed by the software industry were facially challenging to read.[203] Not only were the software licenses and other standard forms unclear, but they were one-sided in favor of industry-stripping warranties and remedies from the licensees or other users. The following section demonstrates how software licensors deploy rights foreclosure clauses such as warranty disclaimers, caps on damages, and arbitration/anti-class action waivers to systematically eliminate U.C.C. Article 2 remedies—leaving the consumer with theoretical rights, but not a minimum adequate remedy. Rights foreclosure clauses are broadly defined as the contractual means those provisions that operationalize the stripping of rights and remedies from software licensees and other users.

a. Warranty Disclaimers

Each of the top ten software companies in the world disclaimed all warranties in their licensing agreements. For example, Apple, a trillion-dollar company,[204] still disclaims all implied warranties in its single user software license agreement. Apple, like Microsoft, offers its services on an "as is" or "with all faults" basis, which means that it disclaims all warranties of quality, including the implied warranty of merchantability

Flesch-Kincaid Readability Calculator. *See Flesch-Kincaid Grade Level Readability Calculator*, https://www.textcompare.org/readability/flesch-kincaid-grade-level [https://perma.cc/S3NZ-3TJH] (last visited Dec. 21, 2023). The Flesch-Kincaid Grade Level test measures readability of passages. *Flesch Reading Ease and the Flesch Kincaid Grade Level*, READABLE, https://readable.com/readability/flesch-reading-ease-flesch-kincaid-grade-level/ [https://perma.cc/HT8C-A8E2] (last visited Dec. 21, 2023) ("The Flesch Kincaid Grade Level is a widely used readability formula which assesses the approximate reading grade level of a text. It was developed by the US Navy who worked with the Flesch Reading Ease. Previously, the Flesch Reading Ease score had to be converted via a table to translate to the reading grade level. The amended version was developed in the 1970s to make it easier to use. The Navy utilised it for their technical manuals used in training. Now it's used for a much wider variety of applications. If a text has a Flesch Kincaid level of 8, this means the reader needs a grade 8 level of reading or above to understand it. Even if they're an advanced reader, it means the content is less time-consuming to read . . . . Flesch readability tests work by taking into account sentence and word counts.").

[203] Michael L. Rustad, *Why a New Deal Must Address the Readability of U.S. Consumer Contracts*, 44 CARDOZO L. REV. 521, 553 Tbl. 5 (2022) (documenting how consumer license and other contracts are drafted at a reading level far beyond the average U.S. consumer).

[204] Samantha Murphy Kelly, *Apple Has Lost $1 Trillion in Market Value in a Year*, CNN BUS. (Jan. 3, 2023, 4:10 PM), https://www.cnn.com/2023/01/03/tech/apple-market-value-decline/index.html [https://perma.cc/HZ9T-G9KW] ("Apple's market cap fell below $2 trillion in trading Tuesday for the first time since early 2021 and one year to the day after the company became the first public tech company valued at $3 trillion.").

and fitness for a particular purpose.[205] Like Microsoft's warranty disclaimer, Apple makes no warranty as to noninterrupted or non-error service.

Apple's warranty disclaimer in its single user contract eliminates liability for accuracy as well as non-infringement, merchantability, and fitness for a particular purpose. Additionally, Apple's Terms and Conditions of Sale imposes a one-year limited liability for all products and services and disclaims both the implied warranty of merchantability and fitness for a particular purpose. Where there is a mandatory consumer rule to the contrary, Apple limits both the duration and remedies for breach.[206]

In eliminating the warranty of merchantability, Apple is telling its customers that it is not willing to entertain minimal claims about whether its software works. Apple does not represent its software as fair, average,

---

[205] U.C.C. § 2-316(3)(b) ("Notwithstanding subsection (2) (a) unless the circumstances indicate otherwise, all implied warranties are excluded by expressions like "as is", "with all faults" or other language which in common understanding calls the buyer's attention to the exclusion of warranties and makes plain that there is no implied warranty.").

[206] Apple no longer has a conspicuous Disclaimer of Warranty clause. Apple now labels its disclaimer clause as "warranty limitations subject to consumer law." The warranty limitations clause states:

> TO THE EXTENT PERMITTED BY LAW, THIS WARRANTY AND THE REMEDIES SET FORTH ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, REMEDIES AND CONDITIONS, WHETHER ORAL, WRITTEN, STATUTORY, EXPRESS OR IMPLIED. APPLE DISCLAIMS ALL STATUTORY AND IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND WARRANTIES AGAINST HIDDEN OR LATENT DEFECTS, TO THE EXTENT PERMITTED BY LAW. IN SO FAR AS SUCH WARRANTIES CANNOT BE DISCLAIMED, APPLE LIMITS THE DURATION AND REMEDIES OF SUCH WARRANTIES TO THE DURATION OF THIS EXPRESS WARRANTY AND, AT APPLE'S OPTION, THE REPAIR OR REPLACEMENT SERVICES DESCRIBED BELOW. SOME STATES (COUNTRIES AND PROVINCES) DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY (OR CONDITION) MAY LAST, SO THE LIMITATION DESCRIBED ABOVE MAY NOT APPLY TO YOU.

Apple One (1) Year Limited Warranty: For Apple Branded Product Only, APPLE, https://www.apple.com/legal/warranty/products/ios-warranty-document-us.html [https://perma.cc/C5UM-9S4F] (last visited Mar. 17, 2024). Apple's limited warranty excludes the warranty of merchantability and fitness for a particular purpose and if there is a mandatory consumer provision to the contrary, Apple limits the duration and remedies for such a breach. *Id.*

or fit for its ordinary purpose of operating as an application.[207] Apple disclaims any warranty which says that its software applications work to operate a computer.

Essentially, Apple is telling its users, "we are not responsible if their products or software fails. Have fun, but if our software does not operate, then stop using the software." Apple's Limited Warranty also disclaims the warranty of fitness for a particular purpose as well as warranties that the software does not contain any hidden vulnerabilities such as code that enables the software giant to remotely prevent user access.

The other nine of the ten largest software companies have functionally similar warranty disclaimers, which disavow responsibility for software vulnerabilities. For the one hundred top software companies, eighty-eight entirely disclaim all of the quality warranties of U.C.C. Article 2, merchantability, and fitness for a particular purpose.

b. Caps on Damages

Nine of the top ten software companies in the world cap a consumer's recovery to a nominal amount. Every software publisher with the exception of Guidewire deploys a cap on damages or liability limitation clause that caps damages to a nominal dollar amount. Adobe's end user license agreement caps damages to the amount paid and disclaims responsibility for all category of damages under any theory of liability.[208]

---

[207] Apple has disclaimed the warranty of merchantability and fitness in its Limited One Year Warranty. What this means is there will be no warranty of merchantability. *See* U.C.C. § 2-314. Merchantability sets minimum quality standards. U.C.C. § 2-314(2) states that for goods to be merchantable, they must be at least such as

(a) pass without objection in the trade under the contract description; and

(b) in the case of fungible goods, are of fair average quality within the description; and

(c) are fit for the ordinary purposes for which such goods are used; and

(d) run, within the variations permitted by the agreement, of even kind, quality and quantity within each unit and among all units involved; and

(e) are adequately contained, packaged, and labeled as the agreement may require; and

(f) conform to the promise or affirmations of fact made on the container or label if any.

UCC §2-314 (2).

[208] *End User License Agreement: ADOBE Software License Agreement*, ADOBE, https://www.adobe.com/products/eula/tools/captivate.html (last visited Dec. 21, 2023).

EXCEPT FOR THE EXCLUSIVE REMEDY OFFERED BY ADOBE ABOVE AND ANY REMEDIES THAT CANNOT BE EXCLUDED OR LIMITED UNDER LAW, ADOBE, ITS AFFILIATES, SUPPLIERS, AND CERTIFICATE AUTHORITIES WILL NOT BE LIABLE TO CUSTOMER

Eighty-nine of the world's largest software companies cap damages to a nominal amount or amount paid foreclosing recovery for all categories of damages: consequential, direct, or punitive. Software consumer licensees were limited to the larger of what they had paid for service for a given period coupled with a nominal amount.[209] The effect of these

> FOR ANY LOSS, DAMAGES, CLAIMS, OR COSTS WHATSOEVER INCLUDING ANY CONSEQUENTIAL, INDIRECT OR INCIDENTAL DAMAGES, ANY LOST PROFITS OR LOST SAVINGS, ANY DAMAGES RESULTING FROM BUSINESS INTERRUPTION, PERSONAL INJURY OR FAILURE TO MEET ANY DUTY OF CARE, OR CLAIMS BY A THIRD PARTY, EVEN IF AN ADOBE REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS, DAMAGES, CLAIMS, OR COSTS. IN ANY EVENT, ADOBE'S AGGREGATE LIABILITY AND THAT OF ITS AFFILIATES, SUPPLIERS, AND CERTIFICATE AUTHORITIES UNDER OR IN CONNECTION WITH THIS AGREEMENT WILL BE LIMITED TO THE AMOUNT PAID FOR THE SOFTWARE, IF ANY. THIS LIMITATION WILL APPLY EVEN IN THE EVENT OF A FUNDAMENTAL OR MATERIAL BREACH OR A BREACH OF THE FUNDAMENTAL OR MATERIAL TERMS OF THIS AGREEMENT. Nothing contained in this agreement limits Adobe's liability to Customer in the event of death or personal injury resulting from Adobe's negligence or for the tort of deceit (fraud). Adobe is acting on behalf of its affiliates, suppliers, and Certificate Authorities for the purpose of disclaiming, excluding and limiting obligations, warranties, and liability, but in no other respects and for no other purpose.

Id.

[209] This finding is drawn from study of liability limitation clauses in the top ten software companies' standard form contracts. Apple, for example, has the following limitation of liability clause that eliminates every conceivable category of damages limiting recovery to the amount a customer has paid in licensing fees:

> EXCEPT AS PROVIDED IN THIS WARRANTY AND TO THE MAXIMUM EXTENT PERMITTED BY LAW, APPLE IS NOT RESPONSIBLE FOR DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY BREACH OF WARRANTY OR CONDITION, OR UNDER ANY OTHER LEGAL THEORY, INCLUDING BUT NOT LIMITED TO LOSS OF USE; LOSS OF REVENUE; LOSS OF ACTUAL OR ANTICIPATED PROFITS (INCLUDING LOSS OF PROFITS ON CONTRACTS); LOSS OF THE USE OF MONEY; LOSS OF ANTICIPATED SAVINGS; LOSS OF BUSINESS; LOSS OF OPPORTUNITY; LOSS OF GOODWILL; LOSS OF REPUTATION; LOSS OF, DAMAGE TO, COMPROMISE OR CORRUPTION OF DATA; OR ANY INDIRECT OR CONSEQUENTIAL LOSS OR DAMAGE HOWSOEVER CAUSED INCLUDING THE REPLACEMENT OF EQUIPMENT AND PROPERTY, ANY COSTS OF RECOVERING, PROGRAMMING, OR REPRODUCING ANY PROGRAM OR DATA STORED IN OR USED WITH THE APPLE PRODUCT OR ANY FAILURE TO MAINTAIN THE CONFIDENTIALITY OF INFORMATION STORED ON THE APPLE PRODUCT.

liability limitations was limiting damages to an amount lower than the filing fee for arbitration,[210] or a filing fee in state,[211] or federal court.[212]

Apple One (1) Year Limited Warranty, *supra* note 206.

Apple's limitation of liability clause eliminates both incidental and consequential damages stemming from a software licensor's breach. Apple has eliminated every category of damages recognized under U.C.C. Article 2. *See* U.C.C. §2-715. A company whose software has crashed due to software vulnerability will have no recovery for any category of damages, other than personal injury or loss of life. Apple's limitation of liability clause states:

> THE FOREGOING LIMITATION SHALL NOT APPLY TO DEATH OR PERSONAL INJURY CLAIMS, OR ANY STATUTORY LIABILITY FOR INTENTIONAL AND GROSS NEGLIGENT ACTS AND/OR OMISSIONS. APPLE DISCLAIMS ANY REPRESENTATION THAT IT WILL BE ABLE TO REPAIR ANY APPLE PRODUCT UNDER THIS WARRANTY OR REPLACE THE APPLE PRODUCT WITHOUT RISK TO OR LOSS OF INFORMATION STORED IN THE APPLE PRODUCT.
>
> SOME STATES (COUNTRIES AND PROVINCES) DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

Id.

See also End User License Agreement:

ADOBE Software License Agreement, ADOBE, https://www.adobe.com/products/eula/tools/captivate.html (last visited Dec. 21, 2023). ("IN ANY EVENT, ADOBE'S AGGREGATE LIABILITY AND THAT OF ITS AFFILIATES, SUPPLIERS, AND CERTIFICATE AUTHORITIES UNDER OR IN CONNECTION WITH THIS AGREEMENT WILL BE LIMITED TO THE AMOUNT PAID FOR THE SOFTWARE, IF ANY.").

[210] The American Arbitration Association's "consumer's administrative fee is capped at $200. The business pays the arbitrator's compensation unless the consumer–post dispute–voluntarily elects to pay a portion of the arbitrator's compensation." *Consumer Arbitration Fact Sheet*, AM. ARBITRATION ASS'N, https://go.adr.org/consumer-arbitration#:~:text=The%20upfront%20cost%20of%20arbitration%20for%20consumer%20claimants,%2410%2C000%2C%20consumer%20claimants%20paid%20an%20average%20of%20%2496 [https://perma.cc/7D2U-F3PQ] (last visited Dec. 21, 2023).

[211] In Massachusetts Superior Court, the filing fee for a complaint if $240 plus a $14 surcharge. *Superior Court Filing Fees*, MASS.GOV, https://www.mass.gov/info-details/superior-court-filing-fees [https://perma.cc/M4MV-3P96] (last visited Dec. 21, 2023) ("filing Fee (each plaintiff): Complaint, Third Party Complaint, Petition or Other Action, Motion to Intervene as Plaintiff (plus $20.00 security fee for each civil case (G.L.c. 262, § 4A) and a $15.00 surcharge (G.L.c. 262, § 4C))").

[212] In Massachusetts federal district court, the cost of filing a Complaint or Notice of Removal is $402. *See Fees, Payments, and Interest Rates*, U.S. DIST. CT.

Apple is one of the few companies that does not cap damages at a nominal amount nor disclaim responsibility for personal injury.[213]

c. Mandatory Arbitration/Class Action Provisions

Chart One: Microsoft's Software Vulnerabilities

Software Vulnerabilities	**Nature of Defect & Impact**	**Numbers of Software Vulnerabilities/**
Denial of Service	"'Denial of service' or 'DoS' describes the ultimate goal of a class of cyberattacks designed to render a service inaccessible."[214]	1,650
Execute Code	"Remote code execution is a cyber-attack whereby an attacker can remotely execute commands on someone else's computing device. Remote code executions (RCEs) usually occur due to malicious malware downloaded by the host and can happen regardless of the device's geographic	3,659

FOR THE DIST. OF MASS., https://www.mad.uscourts.gov/finance/fees.htm [https://perma.cc/76NV-JXJW] (last visited Dec. 21, 2023).

[213] *Repair Terms and Conditions*, APPLE, https://www.apple.com/hk/en/legal/sales-support/terms/repair/generalservice/servicetermsen.html [https://perma.cc/9ZMF-3KJU] (last visited Dec. 21, 2023) ("IF YOU ARE A CONSUMER, YOU MAY HAVE CERTAIN ADDITIONAL RIGHTS WITH REGARD TO SERVICES AND PRODUCTS PROVIDED UNDER THIS AGREEMENT. PLEASE REFER TO YOUR LOCAL CONSUMER AUTHORITY FOR MORE INFORMATION ABOUT YOUR RIGHTS.").

[214] *Denial of Service (DoS) Guidance*, NAT'L CYBER SEC. CENTRE (UNITED KINGDOM), https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection [https://perma.cc/8JBD-AYBP] (last visited Dec. 21, 2023).

	location. Remote Code Execution (RCE) is also referred to as Remote Code Evaluation."[215]	
Overflow	"Given the destructive potential of the flaw, Netgear did not disclose the details, other than saying that it's a pre-authentication buffer overflow vulnerability, which could be used for all kinds of malicious activity, from crashing the device after a denial of service, to arbitrary code execution."[216]	1,527
Bypass Something	"An attacker or unauthorized user can refer to the particular file and thus bypass authorization. Impact to individual organizations depends on many factors that are unique to each organization."[217]	548

[215] *Remote Code Execution (RCE)*, BUG CROWD, https://www.bugcrowd.com/glossary/remote-code-execution-rce/ [https://perma.cc/WU5Y-XSD3] (last visited Dec. 21, 2023).

[216] Sead Fadilpašić, *Netgear Wi-Fi Routers Need to be Patched Immediately*, TECHRADAR PRO (Dec. 30, 2022), https://www.techradar.com/news/netgear-wi-fi-routers-need-to-be-patched-immediately [https://perma.cc/5XBY-6A48].

[217] CAREL *PlantVisor Enhanced Authentication Bypass Vulnerability* (June 29, 2022), https://www.cisa.gov/news-events/ics-advisories/icsa-16-021-01 [https://perma.cc/WC3L-APQK].

Gain Information	"As early as May 2021, the FBI observed Russian state-sponsored cyber actors gain access to an NGO, exploit a flaw in default MFA protocols, and move laterally to the NGO's cloud environment."[218]	729
Gain Privilege	"Privilege chaining vulnerability in acmailer ver. 4.0.2 and earlier, and acmailer DB ver. 1.1.4 and earlier allows remote attackers to bypass authentication and to gain an administrative privilege which may result in obtaining the sensitive information on the server via	663

[218] *Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and 'PrintNightmare' Vulnerability*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (May 2, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-074a [https://perma.cc/G442-N69M] ("After effectively disabling MFA, Russian state-sponsored cyber actors were able to successfully authenticate to the victim's virtual private network (VPN) as non-administrator users and make Remote Desktop Protocol (RDP) connections to Windows domain controllers. The actors ran commands to obtain credentials for additional domain accounts; then using the method described in the previous paragraph, changed the MFA configuration file and bypassed MFA for these newly compromised accounts. The actors leveraged mostly internal Windows utilities already present within the victim network to perform this activity."); *see also Security Vulnerabilities (Information Leak)*, CVE DETAIL, https://www.cvedetails.com/vulnerability-list/opginf-1/gain-information.html [https://perma.cc/G9SY-GCTC] (last visited Dec. 21, 2023).

	unspecified vectors.[219]	
XSS	"Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it."[220]	395
Directory Traversal	With a system vulnerable to directory traversal, an attacker can make use of this vulnerability to step	28

[219] *Security Vulnerabilities (Gain Privilege) (CVSS score >= 9) 44 (CVE-2021-20618)*, CVE Details, https://www.cvedetails.com/vulnerability-list.php?vendor_id=0&product_id=0&version_id=0&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=1&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=9&cvssscoremax=0&year=0&month=0&cweid=0&order=1&trc=6168&sha=2f1f77e26ecf09cf8b4f251b1efc2b4bcad02050 [https://perma.cc/ZK8P-8HJR] (last visited Dec. 21, 2023).

[220] KirstenS, *Cross Site Scripting (XSS)*, OWASP, https://owasp.org/www-community/attacks/xss/ [https://perma.cc/8BBL-HRT6] (last visited Dec. 27, 2023).

	out of the root directory and access other parts of the file system. This might give the attacker the ability to view restricted files, which could provide the attacker with more information required to further compromise the system."[221]	
SQLi Injection	"SQL injection (SQLi) is a cyberattack that injects malicious SQL code into an application, allowing the attacker to view or modify a database."[222]	9
Memory Corruption	"Successful exploitation of this vulnerability in the control systems environment could lead to system processes freezing and potentially allow remote code execution. Impact to individual organizations depends on many	1304

[221] *What is a Directory Traversal Attack?* ACUNETIX, https://www.acunetix.com/websitesecurity/directory-traversal/#:~:text=Directory%20traversal%20or%20Path%20Traversal,the%20web%20server's%20root%20directory.&text=An%20Access%20Control%20List%20is%20used%20in%20the%20authorization%20process [https://perma.cc/9Q88-B7W9] (last visited Dec. 27, 2023).

[222] Bart Lenaerts-Bergmans, *SQL Injection (SQLi): How to Protect Against SQL Injection Attacks*, CROWDSTRIKE (Oct. 10, 2022), https://www.crowdstrike.com/cybersecurity-101/sql-injection/ [https://perma.cc/B6JY-Q6WE].

	factors that are unique to each organization."[223]	
Http Response Splitting	"Successful exploitation of these vulnerabilities could allow an attacker to perform malicious command injection, trick a valid user into downloading malicious software onto their computer. Successful exploitation may also allow an attacker to pose as a legitimate user."[224]	2
CSRF (Cross-Site Request Forgery).	Successful exploitation of this vulnerability allows the ID to be retrieved from the browser and will allow the default ID to be changed. This exploit can cause a loss of power for all attached systems.[225]	9
File Inclusion	"File Inclusion vulnerabilities often affect web applications that rely	1[227]

[223] *Microsoft Remote Desktop Protocol Memory Corruption Vulnerability*, CYBERSECURITY & SEC. INFRASTRUCTURE AGENCY (May 1, 2013), https://www.cisa.gov/news-events/ics-advisories/icsa-12-079-01 [https://perma.cc/R7QM-VVAH]

[224] *Hitachi Energy Modular Switchgear Monitoring* (MSM), CYBERSECURITY & SEC. INFRASTRUCTURE AGENCY (Oct. 5, 2022), https://www.cisa.gov/news-events/ics-advisories/icsa-22-277-02 [https://perma.cc/Y6F8-GNKY].

[225] *XZERES 442SR Wind Turbine CSRF Vulnerability*, CYBERSECURITY & SEC. INFRASTRUCTURE AGENCY (Aug. 27, 2018), https://www.cisa.gov/news-events/ics-advisories/icsa-15-155-01 [https://perma.cc/TLX3-X7UR].

[227] The statistics in this chart are adapted from: *Microsoft Vulnerability Statistics*, *supra* note 167 (using data from the Bar Chart on Vulnerability Type).

	on a scripting run time, and occur when a web application allows users to submit input into files or upload files to the server. They are often found in poorly written applications. File Inclusion vulnerabilities allow an attacker to read and sometimes execute files on the victim server or, as is the case with Remote File Inclusion, to execute code hosted on the attacker's machine."[226]	

Three of the top ten software companies impose predispute mandatory arbitration on their users: Microsoft, Adobe, and Dropbox. Thirty-five of the largest one hundred software companies impose arbitration clauses.[228] Adobe's General Terms of Use couple arbitration with a provision restricting licensees from either initiating or joining class actions.[229] Class actions allow large numbers of software licensees with

[226] Admir Dizdar, *File Inclusion Vulnerabilities: What are They and How do They Work?*, BRIGHT SEC. (June 22, 2021), https://brightsec.com/blog/file-inclusion-vulnerabilities/ [https://perma.cc/U2BJ-6348].

[228] I did a content analysis of the standard form agreements deployed by the 100 largest software companies and found that three of the top ten companies-imposed arbitration. Overall, thirty-five of the one hundred largest software companies required consumers and other users to submit to arbitration.

[229] *Adobe General Terms of Use*, ADOBE (Published Aug. 1, 2022, Effective Sept. 19, 2022), https://www.adobe.com/legal/terms-linkfree.html ("THE MANDATORY ARBITRATION PROVISION AND CLASS ACTION WAIVER IN SECTION 14 (DISPUTE RESOLUTION, CLASS ACTION WAIVER, ARBITRATION AGREEMENT) BELOW GOVERN THE RESOLUTION OF DISPUTES. PLEASE READ THEM CAREFULLY. IF YOU DO NOT AGREE WITH THESE TERMS (AS DEFINED BELOW), INCLUDING THE MANDATORY ARBITRATION PROVISION (IF YOU HAVE NOT OPTED OUT

similar claims to join forces in a single suit to share the expense of litigation.

In defective software cases, class actions allow licensees and other users to bring claims against software vendors where damages are relatively low. Prohibiting licensees and other customers from joining class actions ensures that small damage claims cannot be brought because the filing costs for an individual claim will exceed what can potentially be recovered.[230]

The combination of caps on damages, anti-class action waivers, and forced arbitration ensures that it is not a cost-effective decision for consumers to file an arbitration claim. The empirical study of the world's largest software companies concluded that the vast majority of the top hundred deploy rights foreclosure clauses such as warranty disclaimers and limitation of liability to disavow responsibility for software failure causing either financial or physical injury. Slightly more than one-third required users to waive their judicial rights in favor of a private justice system, notably arbitration.

D. Rights Foreclosure in One Hundred Top Digital Companies

The NYU researchers found that consumers and other users rarely read standard form contracts.[231] This section demonstrates that if consumers read the standard form contracts deployed by the 100 largest digital companies, they would find them to have many rights foreclosure clauses such as warranty disclaimers, caps on damages and mandatory arbitration/anti-class action waivers and other one-sided clauses that systematically divest users of any remedy for software vulnerabilities.

The current state of the law claims that the most successful software and digital companies face no liability for marketing software with known vulnerabilities that enable third party crimes. Through contract law, software makers and assemblers disclaim all warranties and limit liability to a nominal amount. This creative use of contract law reallocates the risk of injuries or damages from defective software to the user community. The result is that the software industry has externalized the costs of making code safe for its intended environment of use onto its end users through one-sided mass-market agreements.

AS ALLOWED HEREIN) AND CLASS ACTION WAIVER, PLEASE DO NOT USE THE SERVICES OR SOFTWARE.").

[230] *Id.* (clause is: 14.2 No Class Actions).

[231] Yannis Bakos et al., *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1, 3 (2014) (finding that consumers rarely read end-user license agreements).

1. Description of Sample of 100 Top Digital Companies

The sample of the one hundred largest digital companies consists of Forbes' Top One Hundred Companies.[232] The ten largest digital companies in the world were Apple, Microsoft, Samsung Electronics, Alphabet-Google, AT&T, Amazon, Verizon, China Mobile, Walt Disney, and Facebook.[233] Thirty-nine of the one hundred companies were headquartered in the U.S.[234] Japan was ranked second in the number of top 100 digital companies headquartered there with thirteen.[235]

The Netherlands and South Korea was ranked third with four companies headquartered in each country there, followed by Canada, Hong Kong, and South Korea (each with three digital companies headquartered there).[236] Germany, India, Switzerland, Taiwan, and the United Kingdom each had two top digital companies in their countries.[237] The remaining digital companies were headquartered in Australia, Finland, Indonesia, Ireland, Mexico, Norway, Saudi Arabia, Spain, Sweden, and the United Arab Emirates with one company each headquartered in their respective countries.[238]

Twenty-six of the one hundred top digital companies specialize in telecommunications.[239] Another eighteen are computer services companies, while fifteen other companies specialize in the business of

---

[232] *Top 100 Digital Companies*, *supra* note 164.

[233] The complete list of digital company names includes Apple – Website, Microsoft, Samsung Electronics, Alphabet - (Google), AT&T, Amazon, Verizon, China Mobile, Walt Disney, Facebook, Alibaba, Intel, Softbank, IBM, Tencent Holdings, NTT, CISCO, Oracle, Deutsche Telekom, Taiwan Semiconductor, KDDI, SAP, Telefónica, América Móvil, Hon Hai Precision, Dell, Orange, China Telecom, SK Hynix, Accenture, Broadcom, Micron, Qualcomm, PayPal, China Unicom, HP, Bel, Tata Consultancy Services, ADP, BT Group, Mitsubishi Electric, Canon, Booking Holdings, Saudi Telecom Company, JD.com, Texas Instruments, Netflix, Phillips, Etisalat, Baidu, ASML Holding, Salesforce, Applied Materials, Recruit Holdings, Singtel, Adobe, Xiaomi, Telstra, Vmware, TE Connectivity, SK Holdings, Murata Manufacturing, Cognizant, NVIDIA, eBay, Telenor, Vodafone, SK Telecom, Vivendi, Naspers, Infosys, China Tower Corp., Swisscom, Corning, Fidelity National Information, Rogers Communication, Nintendo, Kyocera, NXP Semiconductors, Dish Network, Rakuten, Altice Europe, TELUS, Capgemini, Activision Blizzard, Analog Devices, Lam Research, DXC Technologies, Legend Holdings, Lenovo, NetEase, Tokyo Electron, Keyence, Telkom Indonesia, Nokia, Fortive, Ericsson, Fiserv, Fujitsu, and Hewlett Packard Enterprise. *Id.*

[234] *Id.*

[235] *Id.*

[236] *Id.*

[237] *Id.*

[238] *Id.*

[239] *Id.*

semiconductors.[240] The next largest category is software, with seven companies in that category.[241] Six companies are classified as Internet and Catalog Retail, while another six specializing in Electronics.[242] Six companies specialize in Business and Personal Services.[243] Four companies specialize in Broadcasting and Cable.[244]

Three Electrical Equipment companies are in the top one hundred, whereas Recreational and Communications Equipment companies are represented with two each in the digital company study.[245] There iss a single company representing the following areas: Business Financial Services, Consumer Financial Services, Health Care Equipment, and Oil and Gas Operations.[246]

Next, the end user license agreements ("EULA"s) were located, downloaded, and analyzed.[247] For each digital company, basic information was coded on the country in which they are headquartered, what they do (products or services), warranty disclaimers, limitation of liability clauses, arbitration/anti-class action provisions, and choice of law.

2. Rights Foreclosure Clauses in Contracts of Top Digital Companies

a. Warranty Disclaimers

Eighty-six of the top one hundred digital companies in the world disclaim all warranties for their products and services. The top ten digital companies all impose comprehensive warranty disclaimers eliminating the implied warranty of merchantability and fitness or a particular purpose: Apple, Microsoft, Samsung Electronics, Alphabet (Google), AT&T, Amazon, Verizon, China Mobile, Walt Disney, and Facebook. [248]

---

[240] *Id.*

[241] *Id.*

[242] *Id.*

[243] *Id.*

[244] *Id.*

[245] *Id.*

[246] *Id.*

[247] *Id.* These standard form EULAs were analyzed: terms of service, terms of use, service level agreements and other labels.

[248] *Id.* Forbes' list of the top 100 digital companies demonstrates that the term "digital" is much broader than "software" as used in the list of top software companies. *Id.* Digital companies comprise greater diversity in the industries. *Id.* For example, Apple, the number one ranked digital company, is classified in the computer hardware industry. *Id.* Korea's Samsung, the number three ranked digital company, is in the semiconductor industry. *Id.* AT&T, the fifth ranked company is in the telecommunications industry, while Amazon, the sixth ranked company, is an Internet and catalog retail store. *Id.* Walt Disney (the ninth ranked company) is classified in the broadcasting and cable industry, while Facebook, ranked tenth, is a computer

Apple's software license, for example, states that it was providing "the Apple Software and Services . . . 'As Is' and 'As Available' with all faults and without [a] warranty of any kind."[249]

The top digital companies not imposing comprehensive warranty disclaimers tend to be headquartered outside of the United States.[250]

b. Caps on Damages

Eighty-two of the top one hundred digital companies impose hard caps on damages, limiting their liability. The legal effect of the liability limiting provision is to disavow responsibility in paying monetary damages for software vulnerabilities or other breaches of the EULA.

Chart Three below presents the caps on damages for products and services of the ten largest digital companies in the world:

Chart Three: Top Ten Digital Companies' Caps on Damages

Company Name	**Headquarters Location**	**Cap on Damages**
(1) Apple	USA	"In no event shall Apple's total liability to you for all damages (other than as may be required by applicable law in cases involving personal injury) exceed the amount of fifty dollars ($50.00). The

services contract. *Id.* The 100 top digital companies include communication equipment and computer services as well as electronic companies. *See id.*

[249] *Software License Agreement, Single Use License*, APPLE, INC., https://www.apple.com/shop/Catalog/US/Images/singleuser.html [https://perma.cc/V9RC-PQXW] (last visited Dec. 28, 2023) [hereinafter APPLE, *Single Use License*] (at Section 6—Disclaimer of Warranty); *see also Software License Agreements*, APPLE, INC., https://www.apple.com/legal/sla/ [https://perma.cc/RPC6-XZRL] (last visited Dec. 28, 2023) (covering iPad, iPhone, and iPod terms and conditions).

[250] *See e.g.*, *General Terms and Conditions for Purchasing by the DeutscheTelekom Group (GTC Purchasing) Part A: Deutsche Telekom Group Applicable Terms*, DEUTSCHE TELEKOM, www.telekom.com › resource › blob (West Germany); *Terms of Use*, ALTICE EUROPE, https://altice.net/terms-use (Netherlands); *Disclaimer*, CHINA UNICOM, laimerhttps://www.chinaunicom.com.hk/en/global/disclaimer.php (China).

		foregoing limitations will apply even if the above stated remedy fails of its essential purpose."[251]
(2) Microsoft	USA	Capped at $10 or amount equal to the user's Services Fee for the month during which the loss or breach occurred. [252]
(3) Samsung Electronics	South Korea	"…AGGREGATE LIABILITY FOR ALL CLAIMS RELATING TO SPECIFIC SERVICES EXCEED THE AMOUNT YOU PAID US FOR SUCH SPECIFIC SERVICE."[253]
(4) Alphabet/Google	USA	"Google's total liability arising out of or relating to these terms is limited to the greater of (1) $200 or (2) the fees paid to use the relevant services in the 12 months before the dispute"[254]
(5) AT & T	USA	"To the greatest extent permitted by law, our total liability to you (under any legal theory) is a credit or refund that must not exceed the total amount of charges

[251] APPLE, *Single Use License*, *supra* note 249 (at Section 7—Limitation of Liability).

[252] *Microsoft Services Agreement*, *supra* note 118 (at Liability Limitations Clause).

[253] *Samsung Services Terms and Conditions*, SAMSUNG ELECTRONICS CO. (Sept. 30, 2021), https://terms.account.samsung.com/contents/legal/usa/eng/general.html [https://perma.cc/59NP-NBDA] (at Limitation of Liability Clause).

[254] *Terms of Service*, GOOGLE (Jan. 5, 2022), https://policies.google.com/terms?hl=en-US#toc-problems [https://perma.cc/LV5X-9CSA].

		you paid us for the applicable AT&T Service during the shorter of (i) the preceding 24-month period or (ii) the period in which you experienced the issue giving rise to your claims."[255]
(6) Amazon	USA	"unless otherwise required by applicable law, in no event will our or our licensors' aggregate liability with respect to any claim arising from or related to this Agreement or your use of the Amazon Services exceed fifty dollars ($50.00)."[256]
(7) Verizon	USA	"IN NO EVENT SHALL THE MANUFACTURER'S TOTAL LIABILITY TO YOU FOR ALL DAMAGES EXCEED THE AMOUNT PAID FOR THIS LICENSE TO THE SOFTWARE.[257]
(8) China Mobile	China	"CMHK shall not be responsible or liable for any defect in the handsets and/or

[255] *AT&T Consumer Service Agreement*, AT&T, https://www.att.com/legal/terms.consumerServiceAgreement.html. [https://perma.cc/JB5Z-ERD7] (last visited Dec. 28, 2023) (emphasis in the original) (at Limitation of Liability Clause).

[256] *Amazon Services Terms of Use*, AMAZON (Apr. 30, 2021), https://www.amazon.com/gp/help/customer/display.html?nodeId=202140280 [https://perma.cc/4ZK2-Q8EK].

[257] *Consumer Licensing Agreement*, VERIZON, https://www.verizon.com/support/consumer-licensing-agreement/ [https://perma.cc/MY67-4BA7] (last visited Dec. 28, 2023).

		accessory items caused by the warranty and repair thereof or any costs or expenses (including but not limited to delivery or transportation charges) related thereto. In no case shall CMHK owe any duty of care to the Customer in the course of repairing the damaged handsets and/or accessories by the Manufacturer nor shall CMHK be held liable for any direct or indirect consequences in connection with the repair service so rendered by the Manufacturer."[258]
(9) Walt Disney	USA	"IN NO EVENT SHALL OUR TOTAL LIABILITY TO YOU FOR ALL DAMAGES, LOSSES AND CAUSES OF ACTION EXCEED ONE THOUSAND U.S. DOLLARS (US $1,000)."[259]
(10) *Facebook*	USA	"Our aggregate liability arising out of or relating to these Terms or the Meta Products will not exceed the greater of $100 or the amount you

[258] *General Terms & Conditions*, CHINA MOBILE (Dec. 12, 2022), https://eshop.hk.chinamobile.com/en/corporate_information/Customer_Service/contract_terms_conditions/customer-support-t-n-c.html [https://perma.cc/S3ZZ-V84Z].

[259] *Disney Terms of Use*, DISNEY (Sept. 26, 2019), https://disneytermsofuse.com/app/uploads/2019/09/Terms-of-Use_09262019-2.pdf [https://perma.cc/MLB7-5SE8].

		have paid us in the past twelve months."[260]

The ten largest digital companies in the world all imposed caps on damages in their standard form agreements. For the top 100 digital companies, those not imposing caps on damages were disproportionately digital companies located outside the United States. Examples include: China Unicom Global Limited, (Hong Kong),[261] Tata Consumer Products (Mumbai, India),[262] and Telefoni[263] (United Kingdom).

c. Predispute Mandatory Arbitration Clauses

Seven of the top ten digital companies imposed arbitration clauses on their users. Microsoft, Samsung Electronics, Alphabet (Google), ATT, Verizon, China Mobile, Walt Disney, and Facebook. Microsoft's Service Agreement couples binding arbitration and class action waiver terms.[264] Samsung's arbitration clause in its Samsung Galaxy Store Terms and Conditions for User makes it clear that the consumer is waiving their right to a bench or jury trial. Unlike many arbitration agreements in the sample, Samsung has an opt-out procedure.[265] Samsung's arbitration clause applies AAA Commercial Arbitration Rules. Unlike the Microsoft arbitration clause, Samsung does not impose a class action waiver.

Thirty-three of the top 100 digital companies-imposed arbitration on all users, but only two coupled arbitration with anti-class action waivers. Fourteen of the thirty-three companies imposing arbitration were headquartered in the U.S., while five Japanese companies and three Chinese companies included arbitration clauses. In conclusion, the one hundred largest digital companies, like the top software providers, disclaim all warranties and cap damages to a nominal amount. As with

[260] *Facebook Terms of Service*, FACEBOOK, https://www.facebook.com/terms.php [https://perma.cc/8PN8-GMLU] (last visited Dec. 28, 2023) (at 3—Limits on Liability).

[261] *Disclaimer*, CHINA UNICOM GLOB. LTD., (HONG KONG), https://www.chinaunicom.com.hk/en/global/disclaimer.php [https://perma.cc/2DEN-RC76] (last visited Mar. 17, 2024).

[262] *Terms and Conditions*, TATA CONSUMER PRODS., https://www.tataconsumer.com/terms-conditions [https://perma.cc/FED7-PFET] (last visited Mar. 17, 2024).

[263] *Terms and Conditions*, TELEFONI, https://telefoni-eg.com/terms-and-conditions/ (last visited Mar. 17, 2024).

[264] *Microsoft Services Agreement*, *supra* note 118 (at Summary of Arbitration Provisions).

[265] *Samsung Galaxy Store Terms and Conditions for User*, SAMSUNG GALAXY, https://terms.samsungconsent.com/6mztkyy858/TC/1.0/USA/USA_eng.html [https://perma.cc/HN8Y-LE6K] (last visited Dec. 28, 2023) (at 6.8 Dispute Resolution).

the software industry, one in three digital companies impose arbitration on all users foreclosing judicial rights and remedies.

In effect, the largest and most powerful software and digital companies use contract to divest themselves of any responsibility for software vulnerabilities. To paraphrase Woody Allen's character Alvy Singer in the movie *Annie Hall*, the 100 largest software and digital companies deploy standard form contracts somewhere on the continuum between the horrible and the miserable.[266] After generations of this practice, and of the problem getting worse, end users have developed a sort of Stockholm Syndrome with regard to buggy software. They believe it is normal, expected, and inescapable.[267]

IV. PART III. POLICY CHOICES FOR ADDRESSING VULNERABLE SOFTWARE

The recent increase of cybercrime shows no sign of abating, principally because the software industry is releasing vulnerable software into the marketplace that enables the theft of data and trade secrets by state-sponsored and private wrongdoers. This part of the article proposes a federal U.C.C. reform as opposed to tort reforms to address the bad software problem. The first section of Part III critically examines five possible reform proposals addressing President Biden's call for shifting liability for cybersecurity to the software industry, thus enabling users to recover money damages for defective software that causes physical injury, financial harm, or collateral property damage. Civil liability for software industry designers and assemblers whose defectively designed insecure code is the proximate cause of personal or financial injury would thus incentivize safety.[268] The software industry does not implement

[266] "I feel that life is divided into the horrible and the miserable. That's the two categories. The horrible are like, I don't know, terminal cases, you know, and blind people, crippled. I don't know how they get through life. It's amazing to me. And the miserable is everyone else. So, you should be thankful that you're miserable, because that's very lucky, to be miserable." ANNIE HALL (Rollins-Joffe Productions 1977) (quoting the character Woody Allen); *see also* MICHAEL L. RUSTAD, SOFTWARE LICENSING: PRINCIPLES AND PRACTICAL STRATEGIES 292 (Oxford Univ. Press ed., 2010) (comparing this characterization of life by Woody Allen's character to quickwrap license agreements).

[267] Larry Dignan, *Buggy Software: Why Do We Put Up With It?*, ZDNET (July 15, 2010), https://www.zdnet.com/article/buggy-software-why-do-we-put-up-with-it/ [https://perma.cc/6NLL-SAHM].

[268] *See, e.g.*, Michael L. Rustad & Thomas H. Koenig, *Extending Learned Hand's Negligence Formula to Information Security Breaches*, 3 I/S J.L. & POL'Y FOR INFO. SOC'Y 237, 239–40 (2007) [hereinafter Rustad & Koenig, *Extending Learned Hand's Negligence Formula*] (arguing for greater liability for unreasonable data security practices); Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1559 (2005) (liability for

reasonable security in their software products thus enabling cybercriminals to exploit vulnerabilities.[269]

In this section, I propose that Congress should enact a federal reform of U.C.C. warranties as opposed to enacting a tort law solution. Courts are already extending U.C.C. Article 2 warranties to software because warranty damages are recoverable for both economic loss and personal injury.

As explained in an earlier section, the economic loss doctrine and the hundreds of tort reforms undermine the ability of tort law to provide consumers with a meaningful remedy for breach of software contracts.[270]

A. Free-Standing Tort Addressing Software Vulnerabilities

> "*Sui generis* is a Latin expression that translates to 'of its own kind.' It refers to anything that is peculiar to itself; of its own kind or class. In legal contexts, *sui generis* denotes an independent legal classification."[271] An example of free-standing legislation addressing a single issue is the Semiconductor Chip Protection Act.[272]

Sui generis torts causes of action have evolved in the common law. Malicious prosecution, for example, is a *sui generis* recognizing liability for the "filing of a criminal complaint with malice and without probable

---

negligent software design); Michael L. Rustad & Thomas H. Koenig, *Negligent Entrustment for Outsourced Data*, Chapter 6 in DATA PRIVACY AND PROTECTION: ISSUES AND PERSPECTIVES by N. Sudarshan (Amicus Books: ICFAI Univ. (India) Press, 2009); Michael L. Rustad, *Tort of Negligent Enablement of Cyberspace*, Chapter 6 in TORTUOUS LIABILITY by B. Padmashree Rajeshwarrao (Amicus Books: ICFAI Univ. (India) Press, 2009).

[269] Rustad & Koenig, *Extending Learned Hand's Negligence Formula*, *supra* note 268, at 248.

[270] "Just by way of example, state legislatures have enacted hundreds of tort reforms limiting the effectiveness of punitive damages. Most states have taken steps during the last decade to reduce the frequency and size of punitive damage awards. The political struggles over tort reform have created a patchwork of inconsistent regulations which must be carefully monitored. For example, punitive damages are not allowed in the original complaint in Idaho, Illinois, Minnesota, and North Dakota. Colorado, Florida, Illinois, Iowa, Missouri, Oregon and Utah provide that punitive damages be paid partially to a charity or a state fund. Georgia's provision that required punitive damages to be shared with the state treasury was struck down on federal and state constitutional grounds in 1990 as well as its provision allowing only one punitive award of no more than $250,000 to be granted per product." 2 PRODUCTS LIABILITY PRACTICE GUIDE § 19.04 (2023) (State Tort Reforms) (available in Lexis/Nexis).

[271] *Sui Generis*, CORNELL L. SCH. LEGAL INFO. INSTITUTE, https://www.law.cornell.edu/wex/sui_generis [https://perma.cc/G2KP-FE5X] (last visited Dec. 28, 2023).

[272] 1A COMPUTER CONTRACTS § 3A.01 (2022).

cause. The essence of the tort is the wrongful conduct in making the criminal charge."[273] *Sui generis* torts evolve, such as medical malpractice, when "an awareness grows that this is a particular legal area, worthy of its own concepts and considerations."[274]

Part I of this article confirmed that there is growing awareness that defective software leads to security breaches, software failures, and countless other performance issues causing financial, property, personal injury damages, and even death. Yet no common law *sui generis* tort has evolved to address defective software. Neither Congress nor state legislatures require software makers to promptly remediate known vulnerabilities in computer code. If a state statute imposed such a statutory duty, its impact would be limited. Any state statute recognizing a cause of action for inadequate cybersecurity is limited to the borders of the state. The software industry markets their products globally and a state cause of action would apply only to a single jurisdiction.

B. New Tort of Computer Malpractice

To date, courts have not extended the scope of professional negligence beyond a few traditional professions with well-established disciplinary codes. Computer technicians are often highly skilled when deciding whether a computer employee was exempt from the state's overtime wages statute.

The "computer employee" exemption states, in relevant part, that an employee is exempt from overtime wages if the employee is a "computer systems analyst, computer programmer, software engineer, or other similarly skilled worker" whose primary duty is:

(A) the application of systems analysis techniques and procedures, including consulting with users, to determine hardware, software, or system functional specifications;

(B) the design, development, documentation, analysis, creation, testing, or modification of computer systems or programs, including prototypes, based on and related to user or system design specifications;

(C) the design, documentation, testing, creation, or modification of computer programs related to machine operating systems; or

[273] 6A CA JUR ASSAULT AND OTHER WILLFUL TORTS § 379 (4).
[274] 4 MEDICAL MALPRACTICE GUIDE: MEDICAL ISSUES § 79.02 (2023).

(D) a combination of duties described in subparagraphs (A), (B), and (C) the performance of which requires the same level of skills.[275]

Even though computer designers, technicians, and other employees perform highly complex work in selecting or designing computer software and other systems, they are not professionals. A New York Superior Court noted that "[t]o maintain a cause of action for professional malpractice, the defendant must be a professional, a term which courts have found to include doctors, attorneys, engineers, architects and accountants."[276] Every U.S. court has declined to recognize a computer malpractice cause of action.[277]

Courts have yet to recognize computer malpractice as a cause of action. In *PC Connection, Inc. v. IBM*, held that Illinois does not recognize the tort of computer malpractice for computer software systems designers, marketers, and installers.

The attributes of a true profession were highlighted by a New York state court explaining the difference between the professions of law and medicine and other evolving fields that have not evolved as professional disciplines:

> Qualities of professionals liable for professional malpractice include "extensive formal learning and

[275] Friedman v. Nat'l Indem. Co., No. 8:16-CV-258, 2018 WL 1954218, *6–7 (D. Neb. Apr. 13, 2018) (finding that the employee's primary duties constitute exempt work under the "computer employee" exemption of Nebraska's wage overtime statute); 29 U.S.C. § 213(a)(17) (2018).

[276] Condor Cap. Corp. v. Cals Inv'rs, LLC, No. 650034/2019, 2020 WL 1188356, at *17 (N.Y. Sup. Ct. Mar. 11, 2020).

[277] *See, e.g.*, Atkins Nutritionals, Inc. v. Ernst & Young U.S., LLC, 754 N.Y.S.2d 320 (N.Y. App. Div. 2003) (stating that there was no cause of action for professional malpractice by computer consultants); Superior Edge, Inc. v. Monsanto Co., 44 F. Supp. 3d 890, 912 (D. Minn. 2014) (noting that "[o]f the courts to consider the question, the overwhelming majority have determined that a malpractice or professional negligence claim does not lie against computer consultants or programmers," and collecting cases); Heidtman Steel Prods., Inc. v. Compuware Corp., No. 3:97CV7389, 2000 WL 621144, at *13–14 (N.D. Ohio Feb. 15, 2000) (rejecting plaintiff's professional malpractice claim for computer software); Guardian of Ga., Inc. v. Bold Techs. Ltd., No. 1:21 CV 1232, 2022 U.S. Dist. LEXIS 239224, at *11 (N.D. Ohio Jan. 7, 2022) ("Accordingly, here, the court declines to extend a form of computer malpractice to Defendant, and holds that Defendant did not owe a separate duty to Plaintiff outside of their contract."); Batchelar v. Interactive Brokers, LLC, 422 F. Supp. 3d 502, 516 n.4 (D. Conn. 2019) ("What courts have not held, however, is that a claim for professional negligence or 'computer malpractice' exists with respect to the design of computer software."); *see also* Ferris & Salter, P.C. v. Thomson Reuters Corp., 889 F. Supp. 2d 1149, 1150–51 (D. Minn. 2012) ("The Court also observed that 'under Minnesota or Michigan law—no professional negligence action will lie against computer engineers and technicians.'").

> training, licensure and regulation indicating a qualification to practice, a code of conduct imposing standards beyond those accepted in the marketplace and a system of discipline for violation of those standards." . . . In cases alleging professional malpractice, courts have been reluctant to extend the definition of "professional" to professions other than the aforementioned.[278]

Computer scientists and other programmers may be highly skilled, but they do not qualify as professionals because they are not bound by an enforceable code of professional ethics or licensure, which is a requirement for a professional.[279] The essence of a professional standard of care is that courts defer to what is customary. A physician or lawyer is not liable for professional malpractice where they satisfy professional standards of care and exercise professional judgment. In *Coleman v. Deno*,[280] the Louisiana Supreme Court set forth six factors to assist a court in determining whether certain conduct by a qualified health care provider constitutes "malpractice:"

(1) whether the particular wrong is "treatment related" or caused by a dereliction of professional skill;

(2) whether the wrong requires expert medical evidence to determine whether the appropriate standard of care was breached;

(3) whether the pertinent act or omission involved assessment of the patient's condition;

(4) whether an incident occurred in the context of a physician-patient relationship, or was within the scope of activities which a hospital is licensed to perform;

(5) whether the injury would have occurred if the patient had not sought treatment; and

(6) whether the tort alleged was intentional.[281]

---

[278] *Condor Cap. Corp.*, 2020 WL 1188356, at *7.

[279] THOMAS H. KOENIG & MICHAEL L. RUSTAD, GLOBAL INFORMATION TECHNOLOGIES: ETHICS AND THE LAW 30 (West Acad. Publ'g, 2d ed. 2023).

[280] 813 So.2d 303 (La. 2002).

[281] *Id.* at 315–16.

In *Atkins Nutritionals, Inc. v. Ernst & Young, LLP*,[282] Atkins, the creator of a low carb diet plan,[283] entered into an agreement with the accounting firm Ernst & Young, LLP ("E & Y"), in which E & Y was to assist Atkins in selecting a computer accounting system for its new distribution center.[284] In April 2000, E & Y recommended that Atkins acquire a computer software system, Cayenta.[285]

After Atkins Nutritionals experienced numerous problems with the Cayenta computer system, it filed suit in the New York Supreme Court against E & Y and another defendant for computer malpractice.[286] The New York court ruled that the lower court's dismissal of Atkins' computer malpractice cause of action was proper, since that cause of action is not recognized in New York.[287] The court reasoned that E & Y was in the role of a computer consultant and New York does not recognize a malpractice cause of action for computer consultants.[288] The court also observed that E & Y's role in helping him select a computer system for its new distribution center did not constitute either a professional relationship or a fiduciary relationship.[289]

There are many differences between the traditional professionals and the role of computer scientists and other technicians. Legal professionals, like their medical professional counterparts, are not liable for malpractice so long as they satisfy the applicable standard of care.[290] In the traditional professions of law and medicine, expert witness testimony is necessary to establish the standard of care.[291] Both law and medicine require a college degree as well as a graduate professional degree.[292] Both professions have

---

[282] 754 N.Y.S.2d 320 (N.Y. App. Div. 2002).

[283] "The Atkins Diet is a popular low-carbohydrate eating plan developed in the 1960s by heart specialist (cardiologist) Robert C. Atkins. The Atkins Diet restricts carbs (carbohydrates) while focusing on protein and fats. The Atkins Diet has several phases for weight loss and maintenance. It starts out with a very low-carbohydrate eating plan." *Atkins Diet: What's Behind the Claims?* MAYO CLINIC, https://www.mayoclinic.org/healthy-lifestyle/weight-loss/in-depth/atkins-diet/art-20048485#:~:text=The%20Atkins%20Diet%20is%20a,for%20weight%20loss%20and%20maintenance [https://perma.cc/G5VH-CCXK] (last visited Dec. 28, 2023).

[284] *Atkins Nutritionals*, 754 N.Y.S.2d at 321.

[285] *Id.*

[286] *Id.* at 321–22.

[287] *Id.* at 322.

[288] *Id.*

[289] *Id.*

[290] *See, e.g.*, Covil v. Robert & Co. Assocs., 144 S.E.2d 450, 453–54 (Ga. App. 1965).

[291] *Id.*

[292] *See* Eric Cervone, *What is the Bar Exam? The Ultimate Guide to the Bar Exam*, QUIMBEE (Feb. 8, 2022), https://www.quimbee.com/resources/what-is-the-bar-exam-an-ultimate-guide [https://perma.cc/VS3T-C6W7]; Rohan Jotwani, *How Long*

rigorous licensing requirements and are subject to professional discipline.[293] In contrast, computer scientists and other technicians have no formal educational requirements or established standards as in the medical and legal fields.[294]

> To become a physician, training can be ten to twelve years.[295] A doctor must graduate from medical school, pass their boards, and complete a residency that can take five or more years in specialties such as Psychiatry, OB/Gyn, Pediatrics, General Surgery, Anesthesiology, and Orthopedic Surgery.[296] Lawyers too have rigorous mandatory educational requirements in that they must complete a four-year undergraduate program and three years of law school.[297] Some lawyers complete a clerkship after law school and all lawyers must pass a comprehensive bar examination before they are licensed.[298] Massachusetts, for example, requires applicants to complete a two-day exam consisting of a Multistate Performance Test (MPT) and the Multistate Essay Exam (MEE). [299]

In contrast, computer scientists and other designers of software or computer systems do not have a prescribed course of study nor a post-graduate internship or fellowship. Practitioners in computer consulting,

---

Does It Take to Become A Doctor? A Complete Guide, INSPIRA (Oct. 12, 2023), https://www.inspiraadvantage.com/blog/how-long-does-it-take-to-become-a-doctor.

[293] *See* Cervone, *supra* note 292; *see also* Jotwani, *supra* note 292.

[294] KOENIG & RUSTAD, GLOBAL INFORMATION TECHNOLOGIES, *supra* note 279, at 30-31.

[295] Jotwani, *supra* note 292.

[296] *Id.*

[297] To become a licensed attorney in the United States, a person must generally accomplish three things: graduate from an accredited law school, be approved by a state's board of bar examiners (generally known as a "character and fitness" test), and pass a bar examination, typically including the Multistate Professional Responsibility Examination (MPRE). Cervone, *supra* note 292.

[298] *State-by-State Bar Exam Requirements*, AM. U. WASH. COLL. OF L., https://www.wcl.american.edu/academics/academicservices/academic-excellence/bar-exam/survey/ [https://perma.cc/7N7N-GECE] (last visited Dec. 28, 2023) ("Every jurisdiction in the United States sets their own conditions for bar membership, including the format of their bar exam, the application deadlines, and the costs associated with applying for and taking the exam. Because of this wide variety of rules and regulations, it is imperative that every person applying to take the bar exam have a well-informed and complete understanding of the rules for the state where they will take the exam.").

[299] *Id.*

design, and programming are engaged in complex and technically sophisticated activities. However, these activities are not regulated by state licensing laws. Unlike doctors or lawyers, computer scientists cannot be reprimanded, suspended or prohibited from practicing in their field."[300]

Similarly, the Minnesota federal district court ruled that Minnesota does not recognize a computer malpractice cause of action in *Ferris & Salter, P.C. v. Thomson Reuters Corp.*[301] In *Thomson Reuters*, a Michigan law firm filed an action against FindLaw alleging breach of contract and professional negligence stemming from FindLaw's reputed failings in designing and managing its website.[302] Findlaw is an online tool to help sers locate state laws, case law and codes, legal blogs and articles, as well as lawyers and legal services. FindLaw, which features a comprehensive legal directory describes itself as "free, up-to-date, and easily understandable legal information and tools."[303] The Minnesota federal district court refuse to extend malpractice liability to FindLaw reasoning:

> "Because no Minnesota court has held that a malpractice claim may lie against computer consultants and because F&S offers no persuasive reason to deviate from an abundance of authority suggesting that such a claim does not lie, the Court will grant the motion and dismiss the professional negligence claim.[304]

In *Invacare Corp. v. Sperry Corp*.,[305] the federal court for the Northern District of Ohio held that allegations claiming a computer system "failed of its essential purpose" did not new constitute the tort of "computer malpractice" against its manufacturer.[306] It is unlikely that courts or legislatures will recognize computer malpractice as a cause of action for vulnerable software.

This section has demonstrated that courts have refused to apply malpractice liability to computer technicians. U.S. courts have been resistant to classifying computer scientists and other technicians as professionals. Actions against software publishers and computer scientists for other causes of action have been unsuccessful because of the

---

[300] KOENIG & RUSTAD, GLOBAL INFORMATION TECHNOLOGIES, *supra* note 279, at 30.

[301] 889 F. Supp. 2d 1149, 1150 (D. Minn. 2012).

[302] *Id.*

[303] *About Findlaw*, FINDLAW, https://www.findlaw.com/company.html/ [https://perma.cc/U5WZ-FDH4] (last visited Mar. 17, 2024).

[304] 889 F. Supp. 2d 1149, 1150 (D. Minn. 2012).

[305] 612 F. Supp. 448 (N.D. Ohio 1984).

[306] *Id.* at 453–54.

widespread use of warranty disclaimers and other rights foreclosure clauses.[307]

C. Strict Products Liability for Defective Software

"Product liability is the liability of manufacturers, processors, distributors, and sellers of products for personal injury, death, or property damage under diverse theories that include negligence, strict liability, and breach of warranty."[308] "[T]he legal duty of a manufacturer to exercise reasonable care can, in appropriate circumstances, extend beyond the duty not to market a defective product."[309] The basic elements of a strict products liability case are to prove a defect, causation and damages. To recover on a claim of strict liability claim in Maryland for example, a claimant must prove that:

> (1) the product was in defective condition at the time that it left the possession or control of the seller, (2) that it was unreasonably dangerous to the user or consumer, (3) that the defect was a cause of the injuries, and (4) that the product was expected to and did reach the consumer without substantial change in its condition.[310]

"The concept of a 'defect' is one of the defining components of the doctrine of strict products liability, which provides that the manufacturer of a product is liable 'if a defect in . . . its product causes injury while the product is being used in a reasonably foreseeable way.'"[311]

Three types of defect are assertable in a products liability case: (1) manufacturing defect, (2) design defect, and (3) the failure to warn or inadequate warning. [312]

---

[307] Rustad, 38 PEPP. L. REV., *supra* note 70, at 546.

[308] Michael L. Rustad, *Products Liability for Software Defects in Driverless Cars*, 32 S. CAL. INTERDIS. L.J. 171, 209 (2022).

[309] Gilead Tenofovir Cases, 317 Cal. Rptr. 3d 133, 141 (Cal. Dist. Ct. App. 2024).

[310] Casasola v. Jolly Roger Rides, Inc., No. 1:23-cv-02800, 2024 WL 51130, at *2 (D. Md. Jan. 4, 2024) (citing Collins v. Li, 933 A.2d 528 (Md. Ct. Spec. App. 2007)).

[311] *Gilead Tenofovir Cases*, 317 Cal. Rptr. 3d at 145 (quoting Soule v. Gen. Motors Corp., 882 P.2d 298, 302 (Cal. 1994).

[312] "Product liability refers to the liability of manufacturers, processors, distributors, and sellers of products for personal injury or property damage under diverse theories including negligence, strict liability, and breach of warranty. Product liability in a defective software case would be based upon claims that personal injury, death, or property damage was caused by a manufacturing defect, design defect, or failure to warn of a known danger. Courts have been slow to extend product liability to defective software. Liability for software defects is just beginning to evolve, and

It is an unsettled question as to whether products liability should extend to intangibles such as the software incorporated in braking, steering, and other key functions of driverless cars.[313] Motor vehicles are the equivalent of computers on wheel. Software controls many functions of the modern automobile including steering systems, GPS, and brakes.[314] "Autonomous vehicles [(AVs)] incorporate intelligent software algorithms in LiDAR, localization systems, advanced driver assistance systems, power electronics, battery systems, ADAS sensors, and control platforms."[315]

Under my proposed reform, autonomous car makers will be liable for injuries or for deaths caused by defective software.[316] The public policy underlying products liability for defective software was to prevent AV makers from disclaiming or reallocating the risks of defective software components to their customers.[317] Courts have been resistant to stretching strict product liability to defective or vulnerable software; instead, they generally tend to enforce the provider's contractual limits on liability.[318]

Strict liability arguably over-deters by creating too much liability, also deterring the insurance industry from offering policies covering AVs.[319] Another difficulty for courts will be to conceptualize intangible software as a tangible product.[320] The common law has a principle of growth and, to date, no court has held a software maker or assembler strictly liable for defective or vulnerable software.[321] U.S. courts have yet to extend strict liability to third-party software developers, and they are also not accountable because the largest software and digital companies use contract law to reallocate the risk of software vulnerability to users or operators. The next section asks whether designers should be liable for

---

the Principles will jumpstart remedies for consumers harmed by these defects." 1-10 SOFTWARE LICENSING § 10.05 (2016)

[313] Rustad, 32 S. CAL. INTERDIS. L.J., *supra* note 308, at 210.

[314] *Id.* at 183.

[315] *Id.* at 185.

[316] *Id.* at 212.

[317] *Id.* at 213.

[318] Michael L. Rustad & Thomas H. Koenig, *Cybertorts and Legal Lag: An Empirical Analysis*, 13 S. CAL. INTERDISC. L. J. 77, 135–36 (2003) ("Courts have yet to extend products liability theories to bad software, computer viruses, or web sites with inadequate security or defective design."). *See also* DAVID G. OWEN & MARY J. DAVIS, OWEN & DAVIS ON PRODUCTS LIABILITY § 17:30 (Thomson Reuters, 4th ed. 2021) ("Whether manufacturers of computer software should be subject to products liability for personal injuries caused by defective software is an intriguing question. While commentators widely favor the application of products liability theories in such situations, the case law so far is limited to commercial contexts involving claims for economic loss without physical harm.").

[319] OWEN & DAVIS, *supra* note 318.

[320] *Id.*

[321] *Id.*

marketing products with known vulnerability as they are often in the best position to patch or remediate known design defects in their applications and computer systems.

D. Negligent Enablement of Cybercrime

One of the unsettled issues of software liability law is whether a developer or designer should be liable for marketing a product with a defect or vulnerability that enables a third-party cybercriminal to access and exploit a user's computer system. "Tort law is increasingly an institution of social control and public policy, expanding from its traditional role of compensation and reducing the cost of accidents."[322] The software developer, publisher, and designer is almost always the least cost avoider.[323] The software designer is almost always in a better position to identify and remediate vulnerabilities in applications versus the user or systems operator. It is more efficient to detect a vulnerability before a software application is released into the marketplace, where it has the potential of creating catastrophic personal injuries or economic losses.

In a 1995 law review article, my co-author and I proposed that the software industry should be held accountable for inadequately secured software.[324] Since 1995, I have continued to call for the software industry to have civil liability where their defectively designed and insecure code is the proximate cause of personal or financial injury.[325] Insecure or flawed software gives cybercriminals the means to steal data or trade secrets. Despite the foreseeable hazard of insecure software, no U.S. court has recognized tort liability for the negligent enablement of cybercrime as of March 18, 2024.[326] Courts have been slow to find software designers

---

[322] Michael L. Rustad, *Commentary: Smoke Signals from Private Attorney's General in Mega Social Public Policy Cases*, 51 DEPAUL L. REV. 511, 511 (2001).

[323] Broadway Nat'l Bank v. Yates Energy Corp., 631 S.W.3d 16, 37 (Tex. 2021) (Busby, J., dissenting) ("The manufacturer of a product is in the best position to understand and warn users about its risks; in the language of law and economics, those who make products are generally the least-cost avoiders of their risks. By placing the duty to warn on a product's manufacturer, we force it to internalize the full cost of any injuries caused by inadequate warnings—and in that way ensure it is fully incentivized to provide adequate warnings. Subsequent grantees can do nothing to prevent this problem, so there is nothing to gain from making it their burden."); *see also* Holtz v. J.J.B. Hilliard W.L. Lyons, Inc., 185 F.3d 732, 743 (7th Cir. 1999) (explaining that rules should be set to impose contractual liability on the party who is the "least cost avoider"—that is, the party who can avoid the mistake at the lowest cost).

[324] Michael L. Rustad & Lori E. Eisenschmidt, *The Commercial Law of Internet Security*, 10 J. HIGH TECH L. 213 (1995) (this Journal is now the BERKELEY TECH L. J.).

[325] *See e.g.*, *supra* note 268 and accompanying text.

[326] This finding is based on searches of case law files in both Westlaw and Lexis on March 18, 2024. The gist of a negligent enablement claim is to create software

and publishers liable for marketing software with known vulnerabilities that proximately causes personal injury, death, or economic losses.[327]

To recover damages for the proposed tort of the negligent enablement of cybercrime, a plaintiff must prove four elements for the cause of the action: (1) the software company sold, leased or licensed, (2) software in defective condition, (3) the plaintiff sustained either physical or financial injury, and (4) the software defect actually and proximately caused the injury.[328] Neither the courts nor legislatures have defined the level of care for software.[329] No federal statute has defined security standards for software.[330]

The negligent enablement tort for insecure software has yet to evolve. Neither Congress nor the states have enacted statutory standards requiring software makers or assemblers to take prompt remedial measures to address dangerous and costly software vulnerabilities.[331] Another obstacle

---

vulnerabilities that facilitate third party crimes. The concept of enabling liability for industries that facilitate third party crimes and other injuries to third parties was first developed in Robert L. Rabin, *Enabling Torts*, 49 DEPAUL L. REV. 435, 452 (1999) (formulating negligent enablement cause of action against handgun manufacturers for marketing products "'inviting' misuse and consequent harm to innocent victims").

[327] *See id.*; *see also* Rustad & Koenig, 20 BERKELEY TECH. L.J., *supra* note 268 ("[I]t seems unlikely that the courts adopting the Restatement will be receptive to stretching product liability concepts to software, digital information, and other intangibles.").

[328] Rustad & Koenig, 20 BERKELEY TECH. L.J., *supra* note 268, at 1586.

[329] *Id.* at 1593.

[330] *Id.*

[331] The few federal statutes setting a standard of care for security adopt a broad standard of reasonableness as opposed to a more specific set of duties, which makes extant federal standards less useful for a negligence per se determination in a negligent security case. The computer security requirements of the Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996), and the Gramm-Leach-Bliley Act (GLBA), Pub. L. No. 106-102, 501–527, 113 Stat. 1338, 1436–50 (1999) are premised on reasonable security. HIPAA applies to the privacy of medical records and protects all "individually identifiable health information" held or transmitted by a covered entity. 45 C.F.R. § 160.103 (2014). HIPAA's privacy rule prohibits covered entities from using or disclosing individually identifiable information unless authorized by the statute. *Id.* § 164.502(a). The Department of Health and Human Services, which issues privacy and security regulations regarding personal data, has also released rules that require covered entities to safeguard information. *See id.* § 164.530(c)(1). The GLBA creates an affirmative obligation on the part of financial institutions to prevent the disclosure of personal information. 15 U.S.C. § 6802 (2011). The GLBA safeguarding provision requires financial institutions to:

> establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the

to the negligent enablement action is the economic loss doctrine.[332] Because it is a tort action, claims that do not involve property damages other than to the software or physical injury are foreclosed upon by the economic loss rule.[333]

E. Why Tort Law is Not the Solution to the Bad Software Epidemic

1. Economic Loss Rule

In the overwhelming majority of jurisdictions, the economic loss rule prevents plaintiffs from recovering for economic losses in tort.[334] "The economic loss doctrine, . . . bars tort recovery for purely economic losses based on the failure to perform contractual obligations."[335] "The theory behind the economic loss doctrine is that "parties to a contract may allocate their risks by agreement and do not need the special protections of tort law to recover damages caused by a breach of contract."[336] Courts applying the economic loss doctrine to defective software cases would

> security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Id. § 6801(b).

[332] White and Summers' leading treatise on the Uniform Commercial Code notes that for claims of personal injury or death, "tort theories are superior. The damages measures are better: tort law allows recovery for pain and suffering, emotional damages, and punitive damages, none of which are available in contract actions." WHITE ET AL., *supra* note 139, at 196. The economic loss doctrine "generally precludes recovery in tort for economic losses resulting from a party's failure to perform under a contract when the harm consists only of the economic loss of a contractual expectancy." Bradley v. Gatehouse Media Tex. Holdings II Inc., No. 1:22-cv-00304-LY, 2023 WL 2428282, at *4 (W.D. Tex. Mar. 8, 2023) (quoting Texas cases). Under the economic loss doctrine, there can be no enablement or any other tort where the only loss is economics. *Id.* The plaintiff's only recourse is contract where the harm is solely economic loss from a breach of an agreement. *Id.*

[333] Keffer, Inc. v. Golden Eye Tech., LLC, No. 3:23-cv-24-MOC, 2023 WL 2844371, at *2 (W.D.N.C. Apr. 7, 2023) ("North Carolina courts have long limited the circumstances under which an ordinary contract dispute can be transformed into a tort action to preserve contracting parties' legitimate expectations . . . . In other words, where a contract exists between the parties, an action in tort must arise from a violation of a distinct duty to the plaintiff and not a violation of a duty arising purely from the contractual relationship of the parties.") (internal quotations omitted); Hou-Tex, Inc. v. Landmark Graphics, 26 S.W.3d 103, 107 (Tex. App. 2020).

[334] LUIS R. FRUMM & MELVIN I FRIEDMAN, PRODUCTS LIABILITY § 13.07 (Matthew Bender, rev. ed 2023) (Claims for Economic Loss).

[335] Wittmeyer v. Heartland All. for Hum. Needs & Rights, No. 23 CV 1108, 2024 WL 182211, at *3 (N.D. Ill. Jan. 17, 2024).

[336] *Id.*

dismiss cases where the only damages were that the software did not operate as documented.[337]

In *Day v. Advanced Micro Devices, Inc*.,[338] the court dismissed a negligence claim arising out of computer system case because the losses were purely economic as opposed to damages for personal injury or death[339] The economic loss rule in software liability cases will bar all tort claims where the software does not work as intended as it only violates a contractual expectancy.[340] A tort law solution to the defective software problem is hamstrung by the economic loss doctrine. Thus, either a federal or state tort reform solution will leave many victims of vulnerable software without a remedy.

2. Tort Reform Hobbles Tort Remedies for Bad Software

Even if the economic loss doctrine could be bypassed, tort law remedies will be deficient because the vast majority of states have enacted tort reforms limiting plaintiff recovery. "Hundreds of tort reform statutes were enacted in the 1970s and 1980s. Rustad and Koenig have located 262 tort reform statutes of sixteen basic types that were passed in the fifty states and the District of Columbia."[341] Rustad and Koenig found that "restrictions on joint and several liability were passed in thirty states. The

---

[337] "Courts have studiously avoided answering whether software is a "product," and have dismissed most software liability claims by invoking the "pure economic loss" doctrine. Under this rule, no tort recovery may be obtained for losses that are purely financial, and unaccompanied by bodily injury or property damage. The primary rationale for the economic loss doctrine is to police the conceptual border between contract law and tort law. Various justifications have been proffered for maintaining this rigid wall, all of which reduce in essence to skepticisms about intangible injuries, though not necessarily intangible causes." Brian H. Choi, *Crashworthy Code*, 94 WASH. L. REV. 39, 69-70 (2019).

[338] No. 22-cv-04305-VC, 2023 WL 2347421 (N.D. Cal. Mar. 2, 2023).

[339] *Id*. at *1.

[340] Sheen v. Wells Fargo Bank, 505 P.3d 625, 627 (Cal. 2022). The *Sheen* case relied upon in the AT&T case held similarly that the economic loss doctrine forecloses tort reform and the plaintiff has only a contractual remedy. *Id.* (holding the economic loss rule barred the plaintiff's negligence claim and the defendant owed no duty of care to the plaintiff); *see also* Wireless Commc'ns, Inc. v. Epicor Software Corp., No. 3:10CV556-DSC, 2011 WL 90238, at *5 (W.D.N.C. Jan. 11, 2011) (dismissing negligent misrepresentation claim that defendant "tortuously made representations to induce [the plaintiff] to enter into the Agreement" because "at the heart of [the plaintiff's] claim is the performance of the contract."); Hou-Tex, Inc. v. Landmark Graphics, 26 S.W.3d 103, 107 (Tex. App. 2000) (applying economic loss rule rejecting the argument of an oil and gas company that it could proceed against a software developer for negligence, holding that the economic loss doctrine precluded the oil and Gas Company's negligence claims against the software developer).

[341] 2 PRODUCTS LIABILITY PRACTICE GUIDE § 18.08 (2023).

collateral source rule was passed in twenty-two states. Eighty-five medical malpractice reform statutes were passed in forty-five states. Mandatory structured settlement statutes were passed in twenty states."[342]

.

Tort reform is an appealing term that connotes improvements in the civil justice system. The term is more accurately stated as tort deform because the impact is to limit the recovery for injured plaintiffs.[343] The result is that plaintiffs in different jurisdictions have significantly different prospects of recovering. The nonuniformity in state tort remedies makes tort an inefficient mechanism for recovery. "Many tort reforms of the 1970s and 1980s sought to limit the size of punitive damage and noneconomic damage (pain and suffering) awards. The states enacted restrictions in these remedies without serious analysis of their likely impact on the functioning of the tort system."[344]

> State reform has resulted in a tort law hodgepodge, where individual states impose their own limitations on liability, restrictions on the rule of joint and several liability, abolition of the collateral source doctrine, caps on damages, and other restrictions. One unanticipated effect of tort reform is that states have numerous conflicting provisions.[345]

Tort reforms have resulted in large number of procedural rules that are relevant to punitive damages including restrictions on pleading, discovery, jury instructions, caps on punitive damages awards.[346] States have enacted punitive damages reforms mandating jury instructions, ratcheting up standards of review to "clear and convincing" evidence. Limiting the size of punitive damages by a prescribed ratio of punitive to compensatory

---

[342] *Id.*

[343] "The current wave of tort reform has been variously referred to as 'tort deform,' 'tort retrenchment,' 'corporate cost shifting' or 'corporate welfare.' While some would like to depict the recent trend in tort law as a semi-autonomous development in the law to meet the needs of the day, this is not an accurate view. The current wave of tort 'reform' is tied to a systematic and coordinated campaign 'by an army of corporations, foundations, lobbyists, litigation centers, think tanks politicians and academics,' to unmake or undo developments over the last 100 years across the common law." Christopher J. Roederer, *Democracy in America: The Counter-Revolution*, 110 W. VA. L. REV. 647, 677–78 (2008).

[344] Michael L. Rustad, *Nationalizing Tort Law: The Republican Attack on Women, Blue Collar Workers and Consumers'*, 48 RUTGERS L. REV. 673, 733 (1996).

[345] *See* Michael L. Rustad, *The Closing of Punitive Damages' Iron Cage*, 38 LOY. L.A. L. REV. 1297 (2005). In 1986 alone, "1400 tort reform bills were introduced in state legislatures." Rustad, 48 RUTGERS L. REV., *supra* note 344, at 724.

[346] Rustad, 38 LOY. L.A. L. REV., *supra* note 345, at 1367–68.

damages vitiates deterrence because the defendant is able to assess the cost of wrongdoing in advance. Uncapped punitive damages makes the defendant think twice before engaging in a pattern of wrongdoing.[347]

Unlike tort law solutions, U.C.C. Article 2 is not subject to the limitations of tort law's economic loss doctrine nor constrained by the hundreds of state and federal tort reforms that have crippled our civil justice system.[348] Chart Four presents the tort reforms enacted in the states by 2002:

Chart Four: Tort Restrictions Enacted by 2002[349]

Type of Tort Restriction	*Number of States*
Recovery of Punitive Damages	32
Joint & Several Liability Restrictions	35
Prejudgment Interest Restrictions	13
Collateral Source Rule Enacted	22
Non-Economic Damages Restrictions	11
Product Liability Limitations	14
Class Action Restrictions	2
Attorney Retention/Sunshine Provisions	3
Appeal Bond/Reform	9

Tort law in the United States is now composed of a far-from-homogenous patchwork of tort restrictions enacted since the 1970s. Tort law is typically governed by state law, which means that it cannot offer the software industry a consistent or uniform legal framework to address their defective software problems. Fundamental fairness requires that plaintiffs in defective software have minimum adequate remedies for harm, which do not arbitrarily cap justice by limitations on liability. [350]

---

[347] *Id.*

[348] *See generally* David B. Gaebler, *Negligence, Economic Loss, and the U.C.C.*, 61 IND. L.J. 593 (1986); U.C.C. § 2 (AM. L. INST. & UNIF. L. COMM'N 1951).

[349] Michael L. Rustad & Thomas H. Koenig, *Taming the Tort Monster: The American Civil Justice System as a Battleground of Social Theory*, 68 BROOKLYN L. REV. 1, 66–67 (2002).

[350] Rustad, 38 LOY. L.A. L. REV., *supra* note 345, at 1370–1420.

> The American Tort Reform Association (ATRA) is a Washington-DC-based group that was formed in 1986 to represent hundreds of U.S. and foreign

V. PART IV. FEDERAL U.C.C. REFORM TO ADDRESS VULNERABLE SOFTWARE

Neither Congress nor any state legislature has enacted a tort solution creating a duty to remediate vulnerable software or secure databases. Now is the time to reallocate the risks of bad software from the user community back to the least cost avoider by making software warranties nondisclaimable and preventing companies from capping damages at a nominal amount. To achieve this minimum mandatory remedy for defective software, Congress must enact a federal statute prohibiting the use of warranty disclaimers, liability limitations, and arbitration/class action waivers in software and data agreements. Because this reform proposal arms corporations and other entities with a remedy for bad software, it is far less likely to encounter corporate and insurance industry opposition than expanding tort duties.[351] In contrast to tort reform solutions to the software vulnerability problem, U.C.C. Article 2 is relatively uniform like its name suggests. U.C.C. Article 2 does not arbitrarily block recovery as it is not limited by the economic loss doctrine. The proposed reform will directly confront the software industry's pattern and practice of rights foreclosure through warranty disclaimers, caps on damages, and arbitration/class action waivers.

> corporations in their bid to overhaul civil liability laws at the state and national levels. ATRA's members are largely Fortune 500 companies with a direct financial stake in restricting lawsuits. Members have included representatives of the tobacco, insurance, chemical, auto and pharmaceutical industries. Corporate giants like Philip Morris, Dow Chemical, Exxon, General Electric, Aetna, Geico, and Nationwide have all supported ATRA.

Fact Sheet: American Tort Reform Association, CTR. FOR JUST. & DEMOCRACY, https://centerjd.org/content/fact-sheet-american-tort-reform-association [https://perma.cc/S35A-5WZU] (last visited Dec. 28, 2023).

[351] *Impact of Tort Reform on Personal Injury Cases*, JUSTIA, https://www.justia.com/injury/negligence-theory/tort-reform/#:~:text=Tort%20reform%20started%20in%20the%201970s.%20It%20was,public%20perceptions%20and%20legislation%20limiting%20personal%20injury%20lawsuits [https://perma.cc/K2VK-C4SL] (last visited Dec. 28, 2023) ("Tort reform started in the 1970s. It was a movement spearheaded by insurance companies and large corporations, the goal of which was to attack the civil justice system and change rules of law, not through case-by-case adjudication, but through public perceptions and legislation limiting personal injury lawsuits. Those who advocated for tort reform sought to persuade the public that the civil justice system was corrupt and that its operations had adverse effects on the economy. They created advertisements and lobbying campaigns that supported the notion that the judicial process is biased towards plaintiffs, resulting in high liability insurance premiums. Conservative politicians took on this cause, incorporating a change of the civil judicial system into their platforms.").

Software liability would best fit within the legal framework of U.C.C. Article 2—a flexible framework offering uniform remedies for breach of software warranties. Even though the U.C.C. has historically been state law, a federal reform is necessary to assure uniformity and a consistent legal framework for making the software industry accountable for defective software.

The U.C.C. is a familiar legal framework adopted in all fifty-one jurisdictions with relatively few nonuniform amendments. Two U.S. jurisdictions have already invalidated warranty disclaimers in consumer transactions: Massachusetts and Maryland.[352] Massachusetts and Maryland invalidates any disclaimers of either the implied warranty of merchantability or fitness of a particular purpose in a consumer transaction.[353] As a result, all consumer users of software have non-disclaimable rights to fair, average software that is fit for both its ordinary

---

[352] MASS. GEN. LAWS ch. 106, § 2-316A (2023). Massachusetts, for example, does not permit vendors to disclaim the warranty of merchantability nor fitness for a particular purpose. *Id.* Attempted disclaimers in consumer transactions are not enforceable. *Id.* Courts makes disclaimers of consumer sales agreements unenforceable Evans v. Daikin N. Am., LLC, No. 17-10108-RGS, 2019 WL 438340, at *5–6 (D. Mass. Feb. 4, 2019). They invalidate any attempt by a seller to disclaim either the implied warranty of merchantability and fitness for a particular purpose. *Id.* The statutory purpose of this provision is to enable the implied warranties to serve as the functional equivalent of strict products liability. Swartz v. Gen. Motors Corp., 378 N.E.2d 61, 62 (Mass. 1978). Massachusetts is one of the few states, which has never adopted strict product liability. *Id.* Instead, the Commonwealth of Massachusetts deploys Article 2. MASS. GEN. LAWS ch. 106, § 2-316A (2023). To accomplish this result, Section 2-316A prevents sellers from disclaiming either of the implied warranties. *Id.*

[353] As in Massachusetts, Maryland's U.C.C. Article 2 invalidates a seller's attempts to disclaim either of the implied warranties of merchantability or fitness for a particular purpose. MD. CODE ANN., COM. LAW, § 2-316.1 (2011).

MD. CODE ANN., COM. LAW, § 2-316.1 states:

> (1) The provisions of § 2-316 do not apply to sales of consumer goods, as defined by § 9-102, services, or both.
>
> (2) Any oral or written language used by a seller of consumer goods and services, which attempts to exclude or modify any implied warranties of merchantability and fitness for a particular purpose or to exclude or modify the consumer's remedies for breach of those warranties, is unenforceable. However, the seller may recover from the manufacturer any damages resulting from breach of the implied warranty of merchantability or fitness for a particular purpose.

Id.

This section prohibits the use of warranty disclaimers in consumer sales transactions. *Id.*

and particular purpose. In Massachusetts and Maryland, U.S. consumers have mandatory consumer protection functionally equivalent to the European Union's Unfair Contract Terms Directive (UCTD).[354] The Annex to the UCTD considers clauses in consumer transactions that disclaim warranties to be invalid.[355]

The proposed federal commercial law reforms will be a first step to harmonizing consumer law with that of the European Union, our largest trading partner. The Unfair Contract Terms Directive invalidates rights foreclosure clauses in consumer transactions including warranty disclaimers, caps on damages, and arbitration/class actions in the European Union's ("EU") twenty-seven countries.[356] Given that U.S. software companies license their products to the twenty-seven countries of the European Union, this U.C.C. reform will ensure that U.S. software and digital companies comply with the EU's Unfair Contract Terms Directive. U.S. companies, like their European counterparts, will be able to market their products in Europe without facing regulatory action or lawsuits for unfair terms.

The Unfair Contract Terms Directive 93/13/EEC ("UCTD") protects consumers in all countries of the EU from unfair terms and conditions which might be included in a standard form contract for goods and services that they purchase. Article 3 of the UCTD states that the directive applies to all non-negotiated contracts where there is "a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer."[357] The UCTD would apply to the vast

---

[354] Council Directive 93/13/EEC (on unfair terms in consumer contracts) (Apr. 5, 1993).

[355] Part (b) of the Annex to the UCTD strikes down contractual clauses which have the object or effect of:

> (b) inappropriately excluding or limiting the legal rights of the consumer vis-à-vis the seller or supplier or another party in the event of total or partial non-performance or inadequate performance by the seller or supplier of any of the contractual obligations, including the option of offsetting a debt owed to the seller or supplier against any claim which the consumer may have against him;

UNFAIR CONTRACT TERMS DIRECTIVE, Annex at pt. b.

[356] "Under the European Union's Unfair Contract Terms Directive, a court, consumer administrative agency, or a quasi-governmental authority will deploy the Directive to strike down oppressive terms in consumer contracts such as terms of use agreements. European courts question the misplaced assumption that TOU contain bargained for terms. In January 2014, the Berlin Court of Appeals invalidated Facebook's use of Friend Finder and specific provisions of its standard online boilerplate." 1-9 SOFTWARE LICENSING § 9.02 (2016).

[357] Council Directive 93/13/EEC, art. 3, 1993 O.J. (L 095) 29 (EC) (on unfair terms in consumer contracts).

majority of consumer software agreements because relatively few of the them are individually negotiated.[358] The UCTD Annex to Article 3 confirms that the EU would invalidate many provisions in U.S. software consumer agreements including warranty disclaimers, caps on damages, and predispute mandatory arbitration.[359]

Not only will the federal reforms address rights foreclosure clauses—immediately creating meaningful remedies for bad software—but also it will bring U.S. commercial law in alignment with the EU, America's most important trading partner. For the first time in U.S. history, the software industry will be accountable to all licensees (not just consumers) for harm caused by vulnerable software. The proposed U.C.C. federal reform will not just strengthen the rights of users but strengthen national security. To date, software publishers have used warranty disclaimers and caps on damages to systematically strip consumers of any remedy for breach of the license agreements. The proposed federal reform invalidates any attempt of the software industry to use these rights foreclosure or no responsibility clauses to eliminate any meaningful consumer remedy.

VI. PART V: THE SOFTWARE VULNERABILITY CRISIS

A. Biden-Harris Administration's Cybersecurity Strategy

On March 1, 2023, the Biden-Harris Administration released the National Cybersecurity Strategy to secure the full benefits of a safe and secure digital ecosystem for all Americans.[360] President Biden's Cybersecurity Strategy "differs from previous versions in several respects, chiefly by urging far greater mandates on private industry, which controls the vast majority of the nation's digital infrastructure, and by expanding

[358] *Id.* ("A term shall always be regarded as not individually negotiated where it has been drafted in advance and the consumer has therefore not been able to influence the substance of the term, particularly in the context of a pre-formulated standard contract."); *see also* Rustad, 44 CARDOZO L. REV., *supra* note 203, at 575.

[359] Rustad, 44 CARDOZO L. REV., *supra* note 203, at 573. Many of the standard terms in consumer software agreements seek to limit the software publisher's liability. Provision such as warranty disclaimers and caps on damages "exclude of limit liability" of the seller or supplier. *See* Annex to Council Directive 93/13/EEC, art. 3, 1993 O.J. (L 095) 29 (EC) (excluding or limiting the legal liability of a seller or supplier in the event of the death of a consumer or personal injury to the latter resulting from an act or omission of that seller or supplier).

[360] *FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy*, THE WHITE HOUSE (Mar. 2, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/ [https://perma.cc/XCM9-8T92].

the role of the government to take offensive action to preempt cyberattacks, especially from abroad."[361]

President Biden's Cybersecurity Strategy "recognizes that robust collaboration, particularly between the public and private sector, is essential to securing cyberspace."[362] Digital technologies touch every aspect of our lives and create unforeseen risks.[363] "Operating from safe havens like Russia, Iran, and North Korea, ransomware actors exploit poor cybersecurity practices to take control of victim networks and rely on cryptocurrencies to receive extortion payments and launder their proceeds."[364] The U.C.C. is an ideal vehicle for ensuring greater accountability as Article 2 has been adopted in nearly every jurisdiction with relatively few nonuniform amendments.[365] Unlike tort law, U.C.C. Article 2 is a model of uniformity like is name suggests.[366] Rather, it is the Uniform Commercial Code, not a hodgepodge of conflicting provisions such as U.S. tort law.[367]

A second advantage is that the U.C.C. is not encumbered by the economic loss doctrine, which precludes tort causes of action from being asserted when there is no collateral damages or physical injury, only malfunctioning software.[368] Nevertheless, tort litigants in defective software lawsuits can argue that a software vendor violating the federal U.C.C. standard for remediating known software defects can be the basis

---

[361] Sanger, *supra* note 79.

[362] NATIONAL CYBERSECURITY STRATEGY, *supra* note 80, at Introduction.

[363] *Id.* at 2.

[364] *Id.* at 17.

[365] *Uniform Commercial Code by State*, Cornell Univ. Legal Info. Institute, https://www.law.cornell.edu/wex/table_ucc [https://perma.cc/XXD8-GV2A] (last visited Dec. 28, 2023).

[366] U.C.C. § 2 (AM. L. INST. & UNIF. L. COMM'N 1951).

[367] *Id.*; *see also State Tort Reform Enactments*, AM. TORT REFORM ASSOC., https://www.atra.org/resources/state-tort-reform-enactments/ [https://perma.cc/Z9YQ-4DBE] (last visited Dec. 28, 2023).

[368] Gaebler, *supra* note 348, at 641; Eggiman v. Bank of Am., No. 1:22-cv-10298-ADB, 2023 WL 2647071, at *3 (D. Mass. Mar. 27, 2023) (quoting Zoll Med. Corp. v. Barracuda Networks, Inc., 565 F. Supp. 3d 101, 106 (D. Mass. 2021) ("To state a claim for negligence, a plaintiff typically must allege damages beyond pure economic loss, as purely economic losses are unrecoverable . . . in the absence of personal injury or property damage.") (internal quotations omitted); *see also* Moore v. Centrelake Med. Grp., Inc., 299 Cal. Rptr. 3d 544, 561 (Cal. App. 2022) (stating that "there is no recovery in tort for negligently inflicted 'purely economic losses,' meaning financial harm unaccompanied by physical or property damage. The economic loss rule applies, inter alia, where the parties are in contractual privity and the plaintiff's claim arises from the contract (in other words, the claim is not independent of the contract).").

of a *negligence per se* actions.[369] "*Negligence per se* is defined as 'a negligence claim with a statutory or regulatory standard of care substituted for the common law standard of care.'"[370] A federal U.C.C. Article 2 reform which declares that a software or digital company is liable for failing to remediate known software vulnerabilities will also establish a statutory standard of care in *negligence per se* actions for defective software.[371] This proposed reform would advance the Biden-Harris Administration's goal of securing a safe and secure digital ecosystem for consumers, the government, and the business community.

B. Federalizing Consumer Warranties

> There is a precedent for federalizing U.C.C. Article 2 warranty provisions. In 1975, Congress enacted the Magnuson–Moss Warranty Act ("MMWA"), a federal statute enacted to remedy warranty disclosure standards.[372] Congress passed the MMWA to reform warranties and to provide all buyers with the content for uniform warranty labels.[373] The MMWA, like my proposed U.C.C. reforms, is calculated to improve consumer rights. My proposed reform will ensure that consumer licensees will have a minimum adequate remedy, not just uniform warranty language as enacted by the MMWA.[374] Congress called upon the Federal Trade

---

[369] *See* Stewart Baker & Maury Shenk, *A Patch in Time Saves Nine: Liability Risks for Unpatched Software*, 18 CORP. COUNS. 1 (Apr. 2005) (noting that "[a]lthough neither HIPAA nor GLBA provides private individuals with a right to sue, these statutes could have significant weight in private actions under common law").

[370] Alford v. Brooks, 618 F. Supp. 3d 621, 625 (E.D. Ky. 2022).

[371] Gaebler, *supra* note 348, at 642; *see also* Ates v. United States, No. 2:21-cv-00418-JPH-MG, 2023 WL 1765991, at *6 (S.D. Ind. Feb. 2, 2023) ("A claim of negligence per se requires a plaintiff to show that the defendant violated a statute or ordinance without an excuse . . . . The doctrine of negligence per se doesn't concern the duty element of a negligence action; rather, the doctrine assumes the existence of a common-law duty of reasonable care, and the court is asked to adopt the standard of conduct set forth in a statute or ordinance . . . as the standard of conduct required under that preexisting duty, so that a violation of the statute or ordinance serves to satisfy the breach element of a negligence action. In other words, a finding of negligence per se merely represents a judicial acceptance of the legislative judgment that acts in violation of the statute constitute unreasonable conduct.").

[372] 15 U.S.C. §§ 2301–12 (1975).

[373] *Id.*; *see also Businessperson's Guide to Federal Warranty Law*, FED. TRADE COMM'N (Dec. 2006), https://www.ftc.gov/business-guidance/resources/businesspersons-guide-federal-warranty-law [https://perma.cc/VW5P-4YEE].

[374] 15 U.S.C. §§ 2301–12 (1975).

> Commission to formulate regulations implementing the Magnuson-Moss provisions on disclosing consumer warranty terms and conditions, the pre-sale availability of these provisions, and informal settlement procedures.[375]

The MMWA improved U.C.C. warranties by giving consumers minimum mandatory disclosures and more accurate titles for consumer warranties.[376] Congress sought to address three problems with consumer product warranties: (1) the length and complexity of consumer warranties; (2) the use of consumer warranties that are in effect, anti-warranties because they take away far more than they give; and (3) the difficulty of consumers in enforcing warranties particularly where the seller is recalcitrant.[377]

Further federal warranty reform is required to ensure that consumers have meaningful remedies for breach, not just clearer warranty language.

C. Federalization of U.C.C. Article 2

The U.C.C. is a comprehensive commercial code, promulgated by the American Law Institute ("ALI") and the National Conference of Commissioners on Uniform State Law ("NCCUSL"), which began in the early 1940s.[378] Commercial Law in the United States is governed by the

---

[375] *Businessperson's Guide*, *supra* note 373.

[376] *Id.* ("In passing the Magnuson-Moss Warranty Act, Congress specified a number of requirements that warrantors must meet. Congress also directed the FTC to adopt rules to cover other requirements. The FTC adopted three Rules under the Act, the *Rule on Disclosure of Written Consumer Product Warranty Terms and Conditions* (the Disclosure Rule), the *Rule on Pre-Sale Availability of Written Warranty Terms* (the Pre-Sale Availability Rule), and the *Rule on Informal Dispute Settlement Procedures* (the Dispute Resolution Rule) . . . . The Act and the Rules establish three basic requirements that may apply to you, either as a warrantor or a seller: (1) As a warrantor, you must designate, or title, your written warranty as either 'full' or 'limited;' (2) As a warrantor, you must state certain specified information about the coverage of your warranty in a single, clear, and easy-to-read document; (3) As a warrantor or a seller, you must ensure that warranties are available where your warranted consumer products are sold so that consumers can read them before buying. The titling requirement, established by the Act, applies to all written warranties on consumer products costing more than $10. However, the disclosure and pre-sale availability requirements, established by FTC Rules, apply to all written warranties on consumer products costing more than $15.").

[377] Kurt A. Strasser, *Magnuson-Moss Warranty Act: An Overview and Comparison with U.C.C. Coverage, Disclaimer, and Remedies in Consumer Warranties*, 27 MERCER L. REV. 1111 (1976).

[378] BRADFORD STONE, UNIFORM COMMERCIAL CODE XII (West Publ'g Co., 6th ed. 2002).

U.C.C., which is adopted in all fifty-one U.S. jurisdictions.[379] Article 2 of the Uniform Commercial Code applies to transactions in goods and is technically inapplicable to intangibles such as software.[380] U.C.C. Article 2 is, in effect, the chief law governing the sale of goods through the United States.[381]

The goal of the U.C.C. is to "simplify, clarify, and modernize the law governing commercial transactions."[382] U.C.C. Article 2 does not address whether the sale of goods applies to intangible computer code. Article 2 was drafted in the 1950s long before software was conceptualized as a separate product from computer systems.[383] Under the U.C.C., "goods" are "all things (including specially manufactured goods) which are movable at the time of identification to the contract for sale."[384] "While courts have often classified the sale of a software package as a sale of a good for Uniform Commercial Code (U.C.C.) purposes, the applicability of the U.C.C to software as a service (SaaS) and mass-market software licenses is less certain."[385] Software-as-a-Service is rapidly displaced sales and leases. Congress will next need to address greater consumer protection in SaaS contracts. For the foreseeable future, SaaS will evolve further. "SaaS spending is projected to stay strong, reaching 195 billion

---

[379] *Uniform Commercial Code*, UNIF. L. COMM'N, https://www.uniformlaws.org/acts/ucc [https://perma.cc/R3UA-8473] (last visited Dec. 28, 2023).

[380] U.C.C. § 2-102 (AM. L. INST. & UNIF. L. COMM'N 1951).

[381] Uniform Commercial Code Article 2 governs the sale of goods. Uniform Commercial Code, *supra* note 379. It was part of the original Uniform Commercial Code approved in 1951. *Id.* Article 2 represented a revision and modernization of the Uniform Sales Act, which was originally approved by the National Conference of Commissioners on Uniform State Laws in 1906. *Id.* The Uniform Law Commission and American Law Institute approved a revised Article 2 in 2003 that was not adopted in any state, and was subsequently withdrawn by both organizations in 2011. *Id.* Thus, the 1951 version of Article 2 is the most recent official version. *Id.*

[382] *See* U.C.C. §1-103(a) (AM. L. INST. & UNIF. L. COMM'N 2001).

[383] Michael L. Rustad & Elif Kavusturan, *A Commercial Law for Software Contracting*, 76 WASH & LEE L. REV. 775, 789 (2019). The American Law Institute (ALI) and the National Conference of Commissioners on Uniform State Laws (NCCUSL) approved the Uniform Commercial Code (U.C.C.) nearly seventy years ago. *Id.* at 777. The ALI and the NCCUSL approved the original U.C.C. and introduced the model statute in state legislatures throughout the United States. *Id.* "Article 2 of the Uniform Commercial Code, the sales article of the most successful codification in American law, is also the subject of voluminous literature." *Id.* at 778 ((quoting Zipporah Batshaw Wiseman, *The Limits of Vision: Karl Llewellyn and the Merchant Rules*, 100 HARV. L. REV. 465, 466 (1987)).

[384] Oakwood Prods., Inc. v. SWK Techs., Inc., No. 9:20-cv-04107-DCN, 2021 WL 5235224, at *5 (D.S.C. Nov. 10, 2021).

[385] *Id*.

U.S. dollars in 2023."[386] Courts are conflicted as to whether U.C.C. Article 2 applies to software:

> For every court that finds that '[t]he weight of authority favors application of common law and not the U.C.C. with regard to software licenses,' another finds that 'courts nationally have consistently classified the sale of a software package as the sale of a good for U.C.C. purposes.'[387]

"The 2022 amendments to the Uniform Commercial Code address emerging technologies, providing updated rules for commercial transactions involving virtual currencies, distributed ledger technologies (including blockchain), artificial intelligence, and other technological developments."[388] Extending U.C.C. Article 2 to software will update commercial law and allow it to address contracting issues with America's third largest industry. In 2000, the FTC held hearings on consumer software issues, such as warranty provisions, the problem of conspicuous disclosures of material terms, the unavailability of some licenses for presale review, and whether the Magnuson-Moss Act should extend to software.[389] In this section, I have argued that greater and more accurate disclosure of warranty provisions does not go far enough. Consumers need mandatory legislation that ensures that they have nondisclaimable warranties and remedies, which is the thrust of my reform proposal.

---

[386] *Software*, STATISTICA, https://www.statista.com/markets/418/topic/484/software/#overview [https://perma.cc/7A5J-UGR6] (last visited Dec. 28, 2023).

[387] SAS Inst., Inc. v. World Programming Ltd., No. 5:10-25-FL, 2016 WL 3435196, at *10 (E.D.N.C. June 17, 2016) (*compare* Attachmate Corp. v. Health Net, Inc., No. C09-1161 MJP, 2010 WL 4365833, at *2 (W.D. Wash. Oct. 26, 2010) *with* Rottner v. AVG Techs. United States, Inc., 943 F. Supp. 2d 222, 230 (D. Mass. 2013)).

[388] *Uniform Commercial Code*, UNIF. L. COMM'N, https://www.uniformlaws.org/acts/ucc#:~:text=The%202022%20amendments%20to%20the%20Uniform%20Commercial%20Code,%28including%20blockchain%29%2C%20artificial%20intelligence%2C%20and%20other%20technological%20developments [https://perma.cc/43GD-Q7WZ] (last visited Dec. 28, 2023) (at Article 12 and the 2022 Amendments).

[389] I submitted testimony to the Federal Trade Commission's High Technology Warranty Project. My prepared testimony urged Congress to extend the MMWA to mass-market software transactions. Michael L. Rustad (with the assistance of Ronald Kaplan), *Extending Warranty Protection to Cyberspace*, Before the Federal Trade Commission, HIGH TECHNOLOGY WARRANTY PROJECT (Sept. 2000) (cited in 1-5 MICHAEL L. RUSTAD, SOFTWARE LICENSING: PRINCIPLES AND PRACTICAL STRATEGIES (Oxford Univ. Press, 2016) at § 5.13; *see also* Ajay Ayyappan, Note, *UCITA: Uniformity at the Price of Fairness?*, 69 FORDHAM L. REV. 2471, 2520 (2001).

Courts and commentators have debated whether U.C.C. Article 2 covers software licensing as well as hybrid computer contracts that cover services.[390] However, some courts stretch U.C.C. Article 2 to software, even though it is an intangible. A Massachusetts court noted that it was extending Article 2 licensing for a practical concern of clarity and uniformity, in the absence of specialized law for software contracts.[391] Moreover, another reason for applying U.C.C. Article 2 to software is that the U.C.C. is a familiar legal framework that is easily adaptable to rapidly evolving information technologies.

The software industry has found that it is beneficial to extend U.C.C. Article 2 for tangible goods to software code, which is an intangible because of the longer statute of limitations.[392] The Code permits the parties to vary most provisions of U.C.C. Article 2 by agreement.[393] The only limitation is that there are no disclaimers of "good faith, diligence, or reasonableness."[394] Creating a federal cause of action for marketing vulnerable software will eliminate the cannibalization of contract remedies by the software industries. Under my suggestion for federal U.C.C. reforms, software makers, assemblers, and other industry defendants will no longer be able to disclaim warranties, limit liability, or assert a privity defense in a case involving software.

---

[390] *Oakwood Prods., Inc.*, 2021 WL 5235224, at *5 ("While courts have often 'classified the sale of a software package as [a] sale of a good for U.C.C. purposes,' Rottner v. AVG Techs. U.S., Inc., 943 F. Supp. 2d 222, 230 (D. Mass. 2013), the applicability of the U.C.C. to software as a service ("SaaS") and mass-market software licenses is less certain, *see* Rustad & Kavusturan, *supra* note 384, at 822–26 (collecting cases and arguing SaaS and software licensing contracts do not involve tangible goods)."); *see also* I.Lan Sys. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328, 331 (D. Mass. 2002) (stating that "courts in Massachusetts have assumed, without deciding, that Article 2 governs software *licenses*"). *See* Novacore Techs., Inc. v. GST Commc'ns Corp., 20 F. Supp. 2d 169, 183 (D. Mass. 1998), *aff'd*, 229 F.3d 1133 (1st Cir. 1999); VMark Software, Inc. v. EMC Corp., 642 N.E.2d 587, 590 n.1 (Mass. App. 1994); USM Corp. v. Arthur D. Little Sys., Inc., 546 N.E.2d 888, 894 (Mass. App. 1989). *See generally* Lorin Brennan, *Why Article 2 Cannot Apply to Software Transactions*, 38 DUQ. L. REV. 459, 545–77 (2000); Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239, 1244 n.23 (1995).

[391] *I.Lan Sys.*, 183 F. Supp. 2d at 332.

[392] U.C.C. § 2-725(1) (AM. L. INST. 2002) (provides that "[a]n action for breach of any contract for sale [of goods] must be commenced within four years after the cause of action has accrued.").

[393] U.C.C. § 1-102 (AM. L. INST. 2001).

[394] MICH. COMP. L. ANN. § 440.1302(1)–(2) (The Michigan U.C.C., for example, states that "the effect of any provision of this act may be varied by agreement" except that "[t]he obligations of good faith, diligence, reasonableness, and care prescribed by this act may not be disclaimed by agreement."); *see also* Callidus Cap. Corp. v. FCA Grp., No. 14-10484, 2018 WL 1577079, at *11 (E.D. Mich. Mar. 30, 2018).

D. Massachusetts' Elimination of Consumer Warranty Disclaimers

Both software licensors and licensees seek uniform and consistent rules for software and digital information agreements. "Most courts have held that computer software qualifies as a 'good,' but legal uncertainty continues with regard to certain software transactions."[395] Article 2 of the U.C.C. (adopted by all states, except Louisiana) applies to transactions of goods.[396] Massachusetts has decades of experience in eliminating warranty disclaimers for consumer transactions by eliminating horizontal privity in 1971,[397] and recognizing "the fullest possible legal protections to consumers, including a prohibition against the disclaiming by sellers of the implied warranty of merchantability in consumer contracts."[398] Massachusetts' limitation on warranty disclaimers states:

> Any language, oral or written, used by a seller or manufacturer of consumer goods and services, which attempts to exclude or modify any implied warranties of merchantability and fitness for a particular purpose or to exclude or modify the consumer's remedies for breach of those warranties, shall be unenforceable with respect to injury to the person.[399]

Massachusetts has never adopted strict product liability but amending its U.C.C. Article 2 gives plaintiffs a remedy when products fail so it is a functional equivalent.[400] By eliminating privity and making warranties nondisclaimable, Massachusetts prevents sellers of goods from

---

[395] 1 COMPUTER CONTRACTS § 2.02 (2023).

[396] 57 MASS. PRAC. *What Is the UCC?* § 12:1, Westlaw (database updated Dec. 2022).

[397] "Mass. Gen. Laws. ch. 106, § 2-318 was amended in 1971 to abolish the privity rule in breach of warranty cases. In relevant part, the amended statute provides that:

> Lack of privity between plaintiff and defendant shall be no defense in any action brought against the manufacturer, seller, lessor or supplier of goods to recover damages for breach of warranty, express or implied, or for negligence, although the plaintiff did not purchase the goods from the defendant if the plaintiff was a person whom the manufacturer, seller, lessor or supplier might reasonably have expected to use, consume or be affected by the goods.

Organic Mulch & Landscape Supply of New Eng., LLC v. Probec, Inc., No. 16-10658-RGS, 2017 WL 3122561 (D. Mass. July 21, 2017).

[398] Rottner v. AVG Techs. United States, Inc., 943 F. Supp. 2d 222, 226 (D. Mass. 2013)

[399] *Id.* (citing MASS. GEN. LAWS ANN. ch. 106, § 2-316A).

[400] Taupier v. Davol, Inc., 490 F. Supp. 3d 430, 439 (D. Mass. 2020).

disclaiming responsibility for products which cause physical injury or death. Massachusetts is the only jurisdiction which has amended its U.C.C. Article 2 for eliminating the harsh doctrines of privity and disclaimers in consumer transactions. Massachusetts also adopted a nonuniform amendment to U.C.C. Article 2 which provides:

> Any language, oral or written, used by a seller or manufacturer of consumer goods and services, which attempts to exclude or modify any implied warranties of merchantability and fitness for a particular purpose or to exclude or modify the consumer's remedies for breach of those warranties, shall be unenforceable with respect to injury to the person.[401]

The impact of Massachusetts' elimination of privity and making warranties nondisclaimable prevents sellers of goods in that state to disclaim responsibility for products causing physical injury or death. [402] Maryland also precludes sellers from disclaiming the implied warranties of quality in Article 2 consumer transactions.[403] Holding software makers liable for promptly remediating vulnerabilities will reduce the radius of risk for software failure.

With the rapidly evolving Internet of Things, it is difficult to think of products not connected by software. In an era where, for example, vehicles have evolved into "software on wheels," Article 2 warranty disclaimers should not be permitted to undermine public safety. A manufacturer of a conventional vehicle is not permitted to disclaim all legal responsibility for dangerous defects in its vehicles on public policy grounds. The future of the automobile industry will be the software-defined vehicles ("SDVs").[404] Advances in software and semiconductors will enable SDVs to be redesigned with "the electronics and digital architecture to create a continuously evolving platform on wheels, where a software-defined vehicle takes the lead."[405]

---

[401] MASS. GEN. LAWS ANN. ch. 106, § 2-316A (governing the Uniform Commercial Code).

[402] *Id.*

[403] Anthony Pools, a Div. of Anthony Indus., Inc. v. Sheehan, 455 A.2d 434, 436–37 (Md. 1983).

[404] Jeffrey "Jefro" Osier-Mixon, *What's New for Automotive Software in 2022?* RED HAT (Mar. 16, 2022), https://www.redhat.com/en/blog/whats-new-automotive-software-2022 [https://perma.cc/FC99-FTZT] ("The shift to the software-defined vehicle brings forward sophisticated use cases that previous proprietary systems cannot easily accommodate. Through collaboration across the automotive, cloud, IoT computing, and safety communities.").

[405] Haider Ali Khan, *5G, Telematics, and ADAS Will Redefine In-Vehicle Experiences*, MINT (May 28, 2022, 3:25 PM), https://www.livemint.com/auto-

E. Federal Reform Harmonizes U.S. and EU Consumer Law

The federal U.C.C. Article 2 reforms will give corporations, organizations and consumers a cause of action when software vulnerabilities cause physical harm, financial injuries, or collateral property losses. This section makes the case that the federal U.C.C. reforms will harmonize U.S. with EU software consumer transactions. In a 2022 law review article, I argued that rights which are foreclosed in form contracts, in a standardized U.S. style, are:

> unenforceable in the twenty-seven countries of the EU. As such, this Part proposes reforms in U.S. terms of use [ToU], summarized as the "New Deal for Consumer Contracts." The substantive part of this proposal would align U.S. consumer contract law with the EU provisions on unfair and deceptive contracts. These provisions are contained in the EU's Unfair Contract Terms Directive (UCTD), which protects consumers from one-sided terms by imposing a standard of readability that requires contract terms to be drafted in 'plain and intelligible language.'[406]
>
> (a) In Part II of this article, I documented that the top one hundred software companies and the top one hundred digital companies systematically foreclosed any warranties in their disclaimer provisions. Warranty disclaimers and caps on damages are presumptively unfair contract terms under the European Union's Unfair Contract Terms Directive.[407] The Annex strikes down caps on damages and other limitations "of a seller or supplier in the event of the death of a consumer or personal injury to the latter resulting from an act or omission of that seller or supplier."[408]

The UCTD invalidates a large number of commonly encountered terms used by software licensors and digital service providers. The UCTD applies to any consumer contractual term where there is a significant imbalance in favor of the stronger party, such as the software licensors. Consumers in all of the EU countries thus have a statutory remedy against

news/5g-telematics-and-adas-will-redefine-in-vehicle-experiences-11653730863620.html [https://perma.cc/95FR-TX2Z].

[406] Rustad, 44 CARDOZO L. REV., *supra* note 203, at 567.

[407] Council Directive 93/13/EEC, art. 3, 1993 O.J. (L 095) 29, 31 (EC).

[408] *Id.* at 33.

providers that attempt to disclaim all warranties, cap damages to a nominal amount such as $10, or impose predispute mandatory arbitration.

The widespread deployment of warranty disclaimers and liability limitation clauses by the world's largest software and digital companies are presumably unfair in the EU as they are significantly imbalanced "to the detriment of consumers."[409] Predispute mandatory arbitration clauses coupled with class action waivers would also violate the EU's UCTD. Requiring consumers to waive their legal rights in favor of arbitration is a *per se* violation of the UCTD.[410] Software is licensed on a global basis and U.S. companies must follow the consumer law of every country where they do business. The federal U.C.C. reforms will be an important first step towards harmonizing U.S. consumer software law with that of our most important trading partner, the twenty-seven countries of the European Union.

The U.S. software industry is already under siege in the European Union because the European Commission for Competition is rigorously pursuing Big Tech companies for violating EU competition law.[411] Margrethe Vestagr, the EU's Commissioner for Competition "has taken on tech giants Alphabet, Amazon, Apple, and Meta" since becoming Commissioner in 2014. The European Commission imposed a $4.5 billion dollar fine on Alphabet-owned Google, for abuses in the mobile market.[412] Software and digital companies face huge liabilities for violating the Unfair Contract Terms Directive when they market their U.S. style license agreement in Europe. The new federal U.C.C. reforms will be an important first step in Tech Giants revising their standard form agreements to comply with EU consumer law.

F. Private Enforcement Through Private Attorneys General

Private enforcement is a unique American approach enabling private litigants to file suit for a public purpose. Judge Jerome Frank used the term "private attorney general" to refer to "empowering any person, official or not, to institute a proceeding involving such a controversy, even

---

[409] *Id.* at 31.

[410] *Id.* at 33 ("[E]xcluding or hindering the consumer's right to take legal action or exercise any other legal remedy, particularly by requiring the consumer to take disputes exclusively to arbitration not covered by legal provisions, unduly restricting the evidence available to him or imposing on him a burden of proof which, according to the applicable law, should lie with another party to the contract.").

[411] Ayesha Javed, *Margrethe Vestagr*, TIME (Apr. 13, 2023, 6:32 AM), https://time.com/collection/100-most-influential-people-2023/6269855/margrethe-vestager-2023/ [https://perma.cc/RKL2-9PBS].

[412] *Id.*

if the sole purpose is to vindicate the public interest. Such persons, so authorized, are, so to speak, private Attorneys General."[413]

A growing number of digital and software companies understand the importance of private enforcement when it comes to software vulnerabilities. Google uses a bounty system that it calls the "vulnerability reward program" to uncover software vulnerabilities.[414] By February 2023. Google paid out "$12 million for over 2,900 security vulnerabilities."[415] Google reported that it paid $605,000 in a single bounty under its Android Chipset Reward Program and another $468,000 under its Chrome Vulnerability Reward Program.[416] Amazon deploys "Amazon Inspector" which scans for software vulnerabilities in application package dependencies.[417] Amazon has the capacity to scan custom applications for many common vulnerabilities such as injection flaws, data leaks, or problems with encryption.[418] My federal UCC reform will enable software licensees and other users to obtain redress for financial and personal injuries proximately caused by designers that market or fail to remediate software applications with known vulnerabilities. By fortifying U.C.C. warranties and making them nondisclaimable, all users of software will be guaranteed a minimum adequate remedy for breach.

The federal cause of action will enable software users to recover for software vulnerabilities that enable state-sponsored cybercriminals working for Russia, China and North Korea to misappropriate their personal data and trade secrets. Software publishers and designers will no longer be able to deploy contract law to systematically divest users of any

---

[413] Associated Indus. of New York State v. Ickes, 134 F.2d 694, 704 (2d Cir. 1943), *vacated*, 320 U.S. 707 (1943) ("Such persons, so authorized, are, so to speak, private Attorney Generals.").

[414] Hisan Kidawi, *Google's Vulnerability Program Helped Identify 2,900 Security Flaws*, ANDROID HEADLINES (Feb. 27, 2023), https://www.androidheadlines.com/2023/02/google-vulnerability-program-helped-identify-2900-security-flaws.html [https://perma.cc/U8DT-3RWY].

[415] *Id.*

[416] *Id.* ("[T]he Android Vulnerability Program had the highest payout ever of $605,000 for a single report, followed by the Android Chipset Security Reward Program, with $468,000 for more than 700 reports. Google's Chrome Vulnerability Reward Program had an outstanding year, with almost 500 vulnerabilities reported and over $4 million paid in rewards. Late last year, the company also launched the Open Source Software Vulnerability Rewards Program, which had over 100 reports, and paid almost $100,000 in rewards.").

[417] *Amazon Inspector FAQs*, AWS, https://aws.amazon.com/inspector/faqs/?nc=sn&loc=6 [https://perma.cc/7WNV-W7DH] (last visited Dec. 28, 2023).

[418] *Id.*; *see also* Sys. & Method to Check Automation Sys. Project Sec. Vulnerabilities, U.S. Patent No. 11,481,500 B2 (filed Aug. 31, 2018) (issued Oct. 25, 2022).

meaningful remedy. The long-term impact of this reform will be to improve the quality of software, which will strengthen our nation's security as well as economic future.

VII. CONCLUSION

The current state of the law is that billion-dollar software and digital companies have no liability for marketing software with known vulnerabilities that causes financial harm, physical injuries, and collateral property damages to its users. This is not just a case of harm to software licensees, but it is a matter of national security. State-sponsored economic espionage originating from China, Russia, North Korea and other authoritarian countries have been known to exploit software vulnerabilities and to misappropriate valuable U.S. trade secrets. Through contract law, software makers and assemblers disclaim all warranties and limit liability to a nominal amount. This creative use of contract law reallocates the risk of injuries or damages from defective software to the user community. The result is that the software industry has externalized the costs of making code safe for its intended environment of use onto its end users through one-sided mass-market agreements.

Creating a federal cause of action for marketing vulnerable software will eliminate the cannibalization of user's contract remedies by the software industries. Under the federal U.C.C. Article 2 reforms, I propose, software makers, assemblers and other industry defendants will no longer be able to disclaim warranties, limit liability, or compel users to arbitrate their claims and agree to class action waivers. Corporate, organizational, and consumer users will be able to file suit for monetary damages against software and digital companies who market their products with known vulnerabilities that cause collateral property harm, physical injuries, or financial losses.

The net effect of this reform will be the creation of strong incentives for the software industry to take prompt remedial step to mitigate the harm caused by defective software. This reform will not provide meaningful remedies for all software licensees. My U.C.C. federal reforms will create greater incentives for the software industry to engage in greater testing of their products and take prompt remedial measures to remediate software vulnerabilities. Improved software security will also help to thwart economic espionage by state-sponsored cybercriminals.