Indiana Law Journal

Volume 100 | Issue 4 Article 8

6-2025

Moving Slow and Fixing Things

Scott Shackelford
Indiana University Kelley School of Business, sjshacke@iu.edu

Janine Hiller
Virginia Tech, jhiller@vt.edu

Christos Makridis
Arizona State University, christos.a.makridis@gmail.com

Iain Nash
Edge Hill University School of Law, iain.nash@edgehill.ac.uk

Kathryn Kisska-Schulze
Clemson University, kkisska@clemson.edu

See next page for additional authors

Moving Slow and Fixing Things

Authors

Scott Shackelford, Janine Hiller, Christos Makridis, Iain Nash, Kathryn Kisska-Schulze, and Hannibal Travis

Moving Slow and Fixing Things

SCOTT SHACKELFORD,[*] JANINE HILLER,[**] CHRISTOS MAKRIDIS,[***] IAIN NASH,[****] KATHRYN KISSKA-SCHULZE[*****] & HANNIBAL TRAVIS[******]

Silicon Valley, and the U.S. tech sector more broadly, have changed the world in part by embracing a "move fast and break things" mentality popularized by Mark Zuckerberg. While it is true that the tech sector has attempted to break with such a reactive and flippant response to security concerns, including at Microsoft itself through its Security Development Lifecycle, cyberattacks continue at an alarming rate. As a result, there are growing calls from regulators around the world to change the risk equation. An example is the 2023 U.S. National Cybersecurity Strategy, which argues that "[w]e must hold the stewards of our data accountable for the protection of personal data; drive the development of more secure connected devices; and reshape laws that govern liability for data losses and harm caused by cybersecurity errors, software vulnerabilities, and other risks created by software and digital technologies." What exact form such liability should take is up for debate. The defect model of products liability law is one clear option, and courts across the United States have already been applying it using both strict liability and risk utility framings in a variety of cases. This Article delves into the debates by considering how other cyber powers around the world—including the European Union—are extending products liability law to cover software, and it examines the lessons these efforts hold for U.S. policymakers with case studies focusing on liability for AI-generated content and Internet-connected critical infrastructure.

---

[*] Provost Professor of Business Law and Ethics, Indiana University Kelley School of Business; Executive Director, Ostrom Workshop; Executive Director, Center for Applied Cybersecurity Research (CACR).

[**] R.E. Sorensen Professor in Finance and a Professor of Business Law in the Pamplin College of Business, Virginia Tech (retired).

[***] Associate Research Professor at the WP Carey School of Business and Research Affiliate at the Global Security Initiative.

[****] Senior Lecturer in Law at the Edge Hill University School of Law, Criminology, and Policing.

[*****] Associate Professor in the School of Accountancy, Clemson University.

[******] Professor of Law at Florida International University.

INTRODUCTION

Silicon Valley, and the U.S. tech sector more broadly, have changed the world in part by embracing a "move fast and break things" mentality that Mark Zuckerberg popularized[1] but that pervaded the industry long before he founded FaceMash in his Harvard dorm room in 2003. Consider that Microsoft introduced "Patch Tuesday" also in 2003, which began a monthly process of updating buggy code that has now continued for more than a generation.[2] While it is true that the tech sector (along with the U.S. government) has attempted to break with such a reactive and flippant response to security concerns, cyberattacks continue at an alarming rate while the promise of "secure-by-design" has yet to be

1. Hemant Taneja, *The Era of "Move Fast and Break Things" Is Over*, HARV. BUS. REV. (Jan. 22, 2019), https://hbr.org/2019/01/the-era-of-move-fast-and-break-things-is-over [https://perma.cc/9HQQ-8LQS].

2. *See* Tyler Reguly, *The History of Patch Tuesday: Looking Back at the First 20 Years*, FORTRA (Dec. 19, 2023), https://www.tripwire.com/state-of-security/history-patch-tuesday-looking-back-first-20-years [https://perma.cc/PEW7-J7MR].

realized.[3] In fact, given the rapid evolution of artificial intelligence (AI), ransomware is getting easier to launch and is impacting more victims than ever before from car lots to critical infrastructure providers.[4] According to reporting from *The Hill*, criminals "stole more than $1 billion from U.S. organizations in 2023," which is the highest amount on record and represents a 70% increase in the number of victims over 2022.[5] Further, it is not merely cyberattacks that are making the problem of promoting a resilient software ecosystem so vital, with the infamous 2024 CrowdStrike update alone impacting more than eight million Windows machines and causing billions in economic harm, including a $380 million hit to Delta Airlines.[6]

As a result of these alarming trends, there are growing calls from regulators around the world to change the risk equation. An example is the 2023 U.S. National Cybersecurity Strategy, which argues that "[w]e must hold the stewards of our data accountable for the protection of personal data; drive the development of more secure connected devices; and reshape laws that govern liability for data losses and harm caused by cybersecurity errors, software vulnerabilities, and other risks created by software and digital technologies."[7] This sentiment represents nothing less than a repudiation of the "Patch Tuesday" mentality and with it the willingness to put the onus on end users for the cybersecurity failings of software vendors. The Biden administration, instead, promoted a view that shifts "liability onto those entities that fail to take reasonable precautions to secure their software."[8] Lamenting about the need to change the reactive status quo in cybersecurity policy is not unique to the Biden administration; in fact, the calls for a similar change in the risk equation date back at least to the Bush administration, which similarly argued in 2003 for shifting

---

3. *See, e.g.*, Scott J. Shackelford, Craig Jackson, Scott Russell, Emily K. Adams, Anne Boustead & Christos Makridis, *The Difficulties of Defining "Secure-by-Design"*, LAWFARE (Feb. 6, 2024, 8:00 AM), https://www.lawfaremedia.org/article/the-difficulties-of-defining-secure-by-design [https://perma.cc/KE4Q-WPQ7].

4. *See, e.g.*, Megan Cerullo, *CDK Global's Car Dealer Software Still Not Fully Restored Nearly 2 Weeks After Cyberattack*, CBS NEWS, https://www.cbsnews.com/news/cdk-cyber-attack-update-some-systems-restored/ (July 1, 2024, 11:36 AM) [https://perma.cc/A5H2-WVTX].

5. Clayton Vickers, *AI Making Ransomware Easier, More Prevalent, Committee Hears*, THE HILL (Apr. 17, 2024, 10:17 AM), https://thehill.com/homenews/house/4599587-ai-ransomware-easier-committee/ [https://perma.cc/B276-C2HQ].

6. *See* Reinhardt Krause, *Delta CEO: CrowdStrike Compensation from IT Outage Still on Table*, INV.'S BUS. DAILY (Oct. 10, 2024, 9:17 AM), https://www.investors.com/news/technology/crowdstrike-stock-crwd-delta-ceo-compensation-it-outage/ [https://perma.cc/3GND-D2QW]; *It Could Take Up to Two Weeks to Resolve 'Teething Issues' Following CrowdStrike Outage, Clare O'Neil Says*, AUSTL. BROAD. CORP. NEWS, https://www.abc.net.au/news/2024-07-21/microsoft-says-crowdstrike-outage-affected-more-than-8-million/104123326 (July 21, 2024, 2:32 AM) [https://perma.cc/HZH3-UG7S].

7. THE WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY 19 (2023), https://web.archive.org/web/20250116081229/https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [https://perma.cc/KG9E-LD8Q].

8. *Id.* at 20.

the burden of cyberattacks from users to the "most-capable and best-positioned cyber actors."[9]

What exact form such liability should take is up for debate, as it has been for more than two decades; what is changing now, though, is that other cyber powers around the world are aggressively moving forward, creating a largely unprecedented real-world experiment in cybersecurity policy. The defect model of products liability law is one clear option, and courts across the United States have already been applying it using both strict liability and risk utility framings in a variety of cases, including litigation related to accidents involving autonomous Teslas.[10] In considering this idea, here we argue that it is important to learn from the European Union (EU), which has long been a global leader in tech governance, even at the risk of harming innovation, along with the experiences from other leading cyber powers. Most recently, the EU has agreed to reform its Product Liability Directive to include software.[11] When combined with other developments, including transparency initiatives such as the Software Bill of Materials (SBOM), we are seeing a new liability regime crystallize that incorporates principles of accountability, transparency, and secure-by-design.[12] This new regime has major implications both for U.S. firms operating in Europe and for U.S. policymakers charting a road ahead.

The various levers to shape software liability, and more broadly the privacy and cybersecurity landscape, are instructive in at least three ways, each of which is deserving of regime effectiveness research to gauge their respective utility. These include:

1. **Extending Products Liability to Include Cybersecurity Failings:** Following the EU's lead in expanding the definition of "product" to include software and its updates, U.S. policymakers could explore extending traditional products liability to cover losses due to cybersecurity breaches. This would align incentives for businesses to maintain robust cybersecurity practices and offer clearer legal recourse for consumers affected by such failings.
2. **Adopting a "Secure-by-Design" Approach:** New EU legislation, such as the Cyber Resilience Act, mandates that products be secure from the outset. U.S. policy could benefit from similar regulations that require cybersecurity

---

9. Jason Healey, *Twenty-Five Years of White House Cyber Policies*, LAWFARE (June 2, 2023, 9:45 AM), https://www.lawfaremedia.org/article/twenty-five-years-of-white-house-cyber-policies [https://perma.cc/M98L-ZMGA].

10. *See* Chinmayi Sharma & Benjamin C. Zipursky, *Who's Afraid of Products Liability? Cybersecurity and the Defect Model*, LAWFARE (Oct. 19, 2023, 10:24 AM), https://www.lawfaremedia.org/article/who-s-afraid-of-products-liability-cybersecurity-and-the-defect-model [https://perma.cc/M2B9-KSFA].

11. *E.g.*, Oliver Bray, *The EU's Product Liability Directive Expands to Cover Digital Technology*, REYNOLDS PORTER CHAMBERLAIN LLP (Aug. 1, 2024), https://www.rpclegal.com/snapshots/consumer/summer-2024/the-eus-product-liability-directive-expands-to-cover-digital-technology/ [https://perma.cc/SAR4-N4DG].

12. *See, e.g.*, Gina Scinta, *SBOMs Are a Needed Ingredient but Not the Full Recipe for Software Supply Chain Security*, WASH. TECH. (Dec. 13, 2023), https://www.washingtontechnology.com/opinion/2023/12/sboms-are-needed-ingredient-not-full-recipe-software-supply-chain-security/392751/ [https://perma.cc/KA4N-ADSB].

to be an integral part of the design process for all digital products. This would shift some responsibility away from end users to manufacturers, promoting a proactive rather than reactive approach to cybersecurity.

3. **Enhancing Transparency and Accountability Through Regulatory Frameworks:** Inspired by the EU's comprehensive regulatory measures like the General Data Protection Regulation (GDPR) and the AI Act discussed below, the United States could benefit from creating or strengthening frameworks that enforce transparency and accountability in data handling and cybersecurity. Building on the recent guidance from the U.S. Securities and Exchange Commission that requires publicly traded companies to report material cybersecurity incidents within four days, this could include potential requirements for risk assessments, incident disclosures, and a systematic approach to managing cyber risks across all sectors, not just critical infrastructure.

These themes are explored in turn, along with lessons from how other cyber powers are managing threats to critical infrastructure providers, along with the growing prevalence of AI tools and how they are impacting democratic norms and institutions. We argue that secure-by-design is appropriate in considering both cybersecurity and AI systems, but that a one-size-fits-all approach is inappropriate globally and instead should be tailored to the needs of specific sectors and industries. Still, there are baseline cybersecurity protections that should be incentivized and, in some cases, required.[13] To this end, we build from previous work on defining "reasonable" cybersecurity and note how these related efforts should inform resilience in the software ecosystem.[14] We also survey the utility of related tools that are helping to build resilience, including other accountability and transparency initiatives such as SBOM and the Cyber Maturity Model Certification (CMMC) discussed below.

The Article is structured as follows. In Part I, we explore the failure of the "Patch Tuesday" reactive approach to cybersecurity that has been prevalent since before 2003, learning from the history of cybersecurity regulatory and technological failures to date. Part II explores the potential for extending products liability law to software, focusing on the case studies of critical infrastructure and AI-enabled content. Part III features comparative case studies from other leading cyber powers, focusing on the EU. Part IV then distills lessons for policymakers and couches the discussion in the larger discussion of securing democracy in the digital age.

I. THE FAILURE OF REACTIVE CYBERSECURITY

In July 2024, a software update from the cybersecurity firm CrowdStrike caused what has been called the "largest IT outage in history."[15] A bug, or mistake, in the code caused the patch to its Falcon software to crash Windows causing the infamous

13. *See* Shackelford et al., *supra* note 3.

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

15. Brian Fung, *We Finally Know What Caused the Global Tech Outage - and How Much It Cost*, CNN, https://www.cnn.com/2024/07/24/tech/crowdstrike-outage-cost-cause/index.html [https://perma.cc/3Q2G-B839] (July 24, 2024, 7:30 PM).

"Blue Screen of Death."[16] This was not the first time that an update went awry causing such an outage—Kaspersky and even Microsoft itself have caused similar crashes—but what was different here is the scale.[17] Although the myriad costs were still being tallied as of this writing, the insurance industry suggested at least $5 billion in direct losses as a result of the patch with thousands of Delta flights cancelled and the healthcare and banking sectors being especially hard hit at $1.94 and $1.15 billion respectively.[18] Although not a breach in itself, the incident does underscore the importance of instilling effective "incident reporting, business continuity and vendor management practices."[19] It also raises the specter of a proactive cybersecurity posture and the importance of aligned liability structures to encourage the uptake of these best practices.

Despite longstanding interest in proactive cybersecurity, the field has been relatively slow to develop. Early examples from the 2000s, for example, include efforts on the part of the Motion Picture Association of America (MPAA) to contain the problem of piracy by going after the pirates with distributed denial of service (DDoS) attacks, Trojan horses, and rootkits.[20] Other examples abound. From 2003 to 2006, hundreds of "Flash Mobs" targeted fake bank sites that facilitated 419 scams (i.e., advance-fee fraud).[21] These efforts, though, were limited, fragmented, and relatively unsophisticated. The reasons for this situation are manifold but include difficulties of attribution[22] and the fact that cybersecurity was in those times an issue of far less salience and resulting concern to managers and boards of directors contributing to a reactive status quo.[23] More recently, organizations have tried to instill proactive cybersecurity best practices while being mindful of not running afoul of the U.S. Computer Fraud and Abuse Act or other international, federal, and state laws that criminalize the unauthorized access of computer networks.[24]

---

16. Lily Hay Newman, Matt Burgess & Andy Greenberg, *How One Bad CrowdStrike Update Crashed the World's Computer*s, WIRED, https://www.wired.com/story/crowdstrike-outage-update-windows/ (July 20, 2024, 9:30 AM) [https://perma.cc/FK7Z-43YC].

17. *Id.*

18. Fung, *supra* note 15.

19. Sharon Florentine, *CrowdStrike Outage: Legal Experts Weigh in on Liability Implications*, CHANNELE2E (July 23, 2024), https://www.channele2e.com/analysis/crowdstrike-legal-and-liability-implications-as-recovery-progresses [https://perma.cc/S3GV-DT9J].

20. *See* ROBERT ANDERSON, BRIAN LUM & BHAVJIT WALHA, OFFENSE VS. DEFENSE 16 (2005), http://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/OffenseVsDefense.pdf [https://perma.cc/LR9Q-AM4Y].

21. *Flash Mob History*, ARTISTS AGAINST 419, http://wiki.aa419.org/index.php/Flash_Mob_History (Sept. 14, 2010, 11:46 AM) [https://perma.cc/2HH8-XS82].

22. ANDERSON ET AL., *supra* note 20, at 5 (stating that the biggest technical hurdle "is that it is difficult to pin-point the exact source of [an] attack since source addresses can be easily spoofed").

23. For more on this topic, see SCOTT DYNES, CTR. FOR DIGIT. STRATEGIES AT TUCK SCH. OF BUS. AT DARTMOUTH COLL., INFORMATION SECURITY INVESTMENT CASE STUDY: THE MANUFACTURING SECTOR (2006), https://mba.tuck.dartmouth.edu/digital/research/researchprojects/InfoSecManufacturing.pdf [https://perma.cc/J2R5-WH2N].

24. *See* Scott J. Shackelford, Danuvasin Charoen, Tristen Waite & Nancy Zhang,

In general, corporate cybersecurity approaches may be understood to exist along a proactivity spectrum.[25] Many firms remain predominantly reactive.[26] For example, in a 2024 report for the Indiana Executive Council on Cybersecurity that included a survey of 140 organizations from across the state, only 34% of respondents had an updated incident response plan, and "[t]hirty-five percent reported that their organization used an externally developed framework to guide their cybersecurity decision-making," with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) being most popular.[27] These efforts, though, remain insufficient with some 1235 reported data breaches in Indiana in 2023,[28] and reports of global ransomware rates increasing by some 73% in 2023 alone with losses in the billions.[29]

The construction of a more robust and secure software ecosystem is no simple feat. Several federal efforts have been focused on promoting transparency and accountability in the software industry. First, the Software Bill of Materials (SBOM) has emerged as a key building block in software security and software supply chain risk management. A SBOM is "a nested inventory, a list of ingredients that make up software components."[30] While there have not yet been significant legal precedents where companies have been held liable specifically due to SBOM-related issues, regulatory developments suggest that SBOMs could influence future liability considerations. For instance, the U.S. Executive Order 14,028 on Improving the Nation's Cybersecurity mandates federal agencies to require SBOMs from software vendors, aiming to enhance transparency and security in the software supply chain. SBOM work has advanced significantly since 2018 as a collaborative community effort, driven by National Telecommunications and Information Administration

---

Rethinking Active Defense: A Comparative Analysis of Proactive Cybersecurity Policymaking, 41 U. PA. J. INT'L L. 377 (2019); Amanda N. Craig, Scott J. Shackelford & Janine S. Hiller, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52 AM. BUS. L.J. 721 (2015).

25. There are different ways to conceptualize a reactive cybersecurity stance. For example, Scott Dynes, an expert in the economics of information security, has placed companies on proactive-reactive continuums to describe four basic approaches to implementing IT security: the "sore thumb," "IT risk," "business risk," and "systemic" paradigms. DYNES, *supra* note 23, at 9.

26. *See* NICK AKERMAN ET AL., MCAFEE, UNSECURED ECONOMIES: PROTECTING VITAL INFORMATION 8 (2009), https://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf [https://perma.cc/N2RF-58MU] (comparing cybersecurity investment rates across countries) ("It appears that decision makers in many countries, particularly developed ones, are reactive rather than proactive.").

27. Shackelford et al., *supra* note 3.

28. *Indiana Data Breaches*, IND. ATT'Y GEN. CONSUMER PROT. DIV. (2023), https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/files/D-BYear-to-Date-Report-2023.pdf [https://perma.cc/HW43-Z8ZZ].

29. Ryan Chapman, *Ransomware Cases Increased by 73% in 2023 Showing Our Actions Have Not Been Enough to Thwart the Threat*, SANS (Jan. 15, 2024), https://www.sans.org/blog/ransomware-cases-increased-greatly-in-2023/ [https://perma.cc/Y573-2PBU].

30. *Software Bill of Materials (SBOM)*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/sbom [https://perma.cc/F9K6-72E4].

(NTIA)'s multistakeholder process. Originally the brainchild of Allan Friedman, who had served as the Director of Cybersecurity at NTIA, the SBOM concept is going global.[31] Many federal agencies and security vendors are now requiring SBOMs as part of the auditing and approval process, and the idea has spread internationally with calls for a global SBOM standard growing louder.[32]

Like SBOM, the U.S. Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC)[33] is similarly focused on raising cybersecurity preparedness and maturity in the government supply chain. The goal is to require companies doing business with the DoD to meet cybersecurity standards, pegged to the levels of sensitive and national security information that they handle.[34] CMMC 1.0 launched in 2020 identifying five cyber hygiene levels: Basic, Intermediate, Good, Proactive, and Advanced.[35] In November 2021, CMMC 2.0 was introduced in response to complaints about how onerous and expensive it was to attain CMMC 1.0 certification.[36] Specifically, the five levels of cybersecurity readiness were reduced to three, and the assessment and certification process was simplified with self-certification standards at the lower levels.[37] A phased implementation of CMMC 2.0 is expected in late 2025, with DoD contractors and subcontractors being expected to gain compliance by 2028.[38]

These efforts at boosting supply chain security for both software and hardware are informed by well-known security principles such as security-by-design. This is not a new concept; some maintain that it dates back to at least the 1970s.[39] Various companies, including Microsoft through its Security Development Lifecycle, have tried to implement security-by-design with varying degrees of success during the preceding decades.[40] Yet recent events, including the July 2024 CrowdStrike fiasco

---

31. *See* Eric Braun, *Wanted: An SBOM Standard to Rule Them All*, DARK READING (July 23, 2024), https://www.darkreading.com/vulnerabilities-threats/wanted-sbom-standard-to-rule-them-all [https://perma.cc/59FK-LU3W].

32. *See id.*

33. *See* Cyber Insights Team, *Department of Defense Unveils CMMC 2.0, Opening a Five-Year Implementation Window*, SEC. BOULEVARD (Jan. 25, 2022) [hereinafter CMMC 2.0], https://securityboulevard.com/2022/01/department-of-defense-unveils-cmmc-2-0-opening-a-five-year-implementation-window-apptega/ [https://perma.cc/M8DV-L4PD].

34. Press Release, U.S. Dept. of Defense, Cyber Security Maturity Model Certification Program Final Rule Published (Oct. 11, 2024) (requiring an assessment and contractual implementation).

35. CMMC 2.0, *supra* note 33.

36. *See Strategic Direction for Cybersecurity Maturity Model Certification (CMMC) Program*, U.S. DEP'T OF DEF. (Nov. 4, 2021), https://www.defense.gov/News/Releases/Release/Article/2833006/strategic-direction-for-cybersecurity-maturity-model-certification-cmmc-program/ [https://perma.cc/7GGT-VDMJ].

37. CMMC 2.0, *supra* note 33.

38. *Id.*

39. Jim Perkins, *Secure by Design Ensures Cyber Security Is No Longer an Afterthought*, BUS. AGE (Oct. 17, 2023), https://www.businessage.com/post/secure-by-design-ensures-cyber-security-is-no-longer-an-afterthought [https://perma.cc/6C4K-DE68].

40. *See Security Development Lifecycle (SDL) Practices*, MICROSOFT, https://www.microsoft.com/en-us/securityengineering/sdl/practices [https://perma.cc/RJR4-3NT8].

mentioned above, along with security failings in Microsoft Exchange highlighted in a Cyber Safety Review Board report, highlight how far the industry still has to go.[41] In response, the Biden administration released a National Cybersecurity Strategy in 2023 in which it called on Congress to promote the adoption of security-by-design principles, which the Cybersecurity and Infrastructure Security Agency defines as a product in which "the security of [the] customers [is] a core business requirement," not an afterthought or technical feature.[42] The current notion of security-by-design builds off of several related initiatives, including zero trust security.

In May 2021, the Biden administration called for the adoption of zero trust security by the federal government.[43] Trust in the context of computer networks refers to systems that allow people or other computers access with little or no verification of who they are and whether they are authorized to have access. Zero trust, by contrast, is a security model that takes for granted that threats are omnipresent inside and outside networks. Zero trust instead relies on continuous verification via information from multiple sources. In doing so, this approach assumes the inevitability of a successful cyberattack. Instead of focusing exclusively on preventing breaches, zero trust security ensures that damage is limited and that the system is resilient and can recover quickly. Yet getting organizations ready for a zero-trust approach, particularly those with legacy systems and the technical debt that goes along with them, requires significant investment and leadership.

In sum, there remains a diversity of organizational approaches to cybersecurity, although organizations with coordinated, centralized, and proactive cybersecurity policies managed by effective leaders fare better than those with a more reactive stance. Tools like SBOM and CMMC 2.0, along with concepts like secure-by-design and zero trust security, can help leaders better understand and manage the cyber threats facing their organizations. This may broadly be considered as an application of the power of negative thinking to cybersecurity, for example, to plan for every possible type of cyberattack and thereby gain knowledge about the strengths and weaknesses in a firm's cybersecurity strategy.[44]

---

41. *See Cyber Safety Review Board Report on Summer 2023 Microsoft Online Exchange Incident*, CISA, https://www.cisa.gov/resources-tools/resources/cyber-safety-review-board-releases-report-microsoft-online-exchange-incident-summer-2023 [https://perma.cc/V2NQ-PFSA].

42. *Secure by Design*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/securebydesign [https://perma.cc/YBW2-DQBR].

43. Joseph R. Biden, *Executive Order on Improving the Nation's Cybersecurity*, THE WHITE HOUSE (May 12, 2021), https://web.archive.org/web/20250119085114/https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ [https://perma.cc/5R4W-Y8AF].

44. *See* CHRIS HADFIELD, AN ASTRONAUT'S GUIDE TO LIFE ON EARTH 53–54, 72 (2013) ("Like most astronauts, I'm pretty sure that I can deal with what life throws at me because I've thought about what to do if things go wrong, as well as right. That's the power of negative thinking.").

II. PROMOTING ACCOUNTABILITY IN THE SOFTWARE ECOSYSTEM

The CrowdStrike-induced outage led to a bevy of high-profile finger-pointing among Delta Airlines—which lost more than $380 million following days of outages and disruptions—Microsoft, and CrowdStrike about which firm was most responsible for the disruptions.[45] The fiasco is unpacked further in Section II.B, but at issue is a clause in the contract between CrowdStrike and Delta that reportedly limits CrowdStrike's liability to the "single-digit millions," another sign of the lack of accountability—and transparency—in the software security supply chain.[46] The question of where liability should rest, how it should be apportioned as a matter of policy, and what—if any—guardrails Congress and state legislatures should place on tech firms and their clients has become a hot topic. Relatedly, cyber risk insurance coverage, which has become pressing following acts of war and hostile acts exclusions in many policies,[47] has emerged as a new battle line in this dispute particularly related to errors and omissions (E&O) insurance given the faulty software update in question.[48]

The options for promoting accountability and transparency in the software ecosystem are numerous and extend beyond products, although that remains the primary focus of this Article. In brief, they include the following legal tools and mechanisms summarized in Table 1 along with some of the most relevant policy benefits and drawbacks. Regime effectiveness studies across many of these tools remain nascent. One exception is cyber risk insurance, which is better studied than other areas in part because of the amount of money on the line after high-profile breaches.[49]

---

45. *See, e.g.*, Alison Sider, *CrowdStrike to Delta: Stop Pointing the Finger at Us*, WALL ST. J. (Aug. 4, 2024, 10:06 PM), https://www.wsj.com/business/airlines/crowdstrike-to-delta-stop-pointing-the-finger-at-us-5b2eea6c [https://perma.cc/KVV8-BZNV].

46. *Id.*; *see CrowdStrike Software Terms of Use*, CROWDSTRIKE, https://www.crowdstrike.com/software-terms-of-use/ [https://perma.cc/FW76-RFXB]; *infra* note 84 and accompanying text.

47. *See* Scott J. Shackelford, *Wargames: Analyzing the Act of War Exclusion in Insurance Coverage and Its Implications for Cybersecurity Policy*, 23 YALE J.L. & TECH. 362, 362 (2021).

48. *See* Florentine, *supra* note 19.

49. *See, e.g.*, Darren Pain, *Cyber Risk Accumulation: Fully Tackling the Insurability Challenge*, GENEVA ASS'N (Nov. 2023), https://www.genevaassociation.org/sites/default/files/2023-11/cyber_accumulation_report_91123.pdf [https://perma.cc/2BRW-3LDD].

Table 1: Legal & Policy Tools for Improving Accountability in the Software Ecosystem

Legal & Policy Tool	**Benefit(s)**	**Drawback(s)**
Contractual Provisions	Honor freedom of contract; promotes flexibility due to changing technological and regulatory circumstances.	Contracts of adhesion leading to inequity and one-sided terms.
Insurance	Market-based approach; variety of policies available to limit liability for various types of cyber risks.	E&O software coverage is questionable, along with other exclusions, limits applicability; rising cost and geographic availablility outside of the United States, United Kingdom, and Germany remains limited.
Products Liability	Clarity along with long-established precedent in other contexts means that courts have myriad tools to apply this corpus of law to the online context.	Concerns about how the extension could impact open-source software communities, along with the increasing cost of software and impacts on innovation.
Tort	Flexibility of common law to apply to new contexts including software, and ability to rely on flexible standards such as reasonable care.	The economic loss doctrine, and other limitations such as in the disclosure requirements of privacy torts limit their efficacy.
Antitrust	Recent U.S. government wins such as in the Google case show that antitrust laws can be applied to reign in monopolostic behavior in the tech sector. They have also been used against Facebook to limit unnecessary app and website data harvesting, centralizing, and sharing, and purchases of offline consumer data to promote	Outdated U.S. antitrust statutes provide more limited ability of U.S. policymakers to reign in abuses compared to EU counterparts. Further, they may threaten cybersecurity as noted by Apple and NetChoice in opposition to (a) Epic Games' proposed antitrust and California law remedy and (b) laws like the AOICA

	online-offline dossiers as noted in FCO / BKA v. Facebook, Zuboff, etc.	(Klobuchar) and Open App Markets Act (Blumenthal and Blackburn etc.) and (in EU) Digital Markets Act or Commission v. Apple (Music) or Commission v. Apple (Apple Pay).
Tax Code	Widely recognized carrot for incentivizing the uptake of best practices in different fields.[50]	Can be a clumsy tool to promote reasonable cybersecurity if it is not tailored to different firm types and resource endowments.
International Agreements	Wide-reaching, coalition building.	Can be difficult to enforce commitments.
Federal & State Constitutional Provisions	Provide overarching protections across sectors and use cases.	Subject to judicial interpretation.

The following Sections unpack these policy options in more detail, beginning with products liability. One of the primary reasons that we chose to focus on products liability in particular is the relative paucity of studies delving into the efficacy of this approach to buttressing software resilience. It is also important to note that there are no bright lines between these various policy tools and legal regimes. In practice, significant overlap exists, such as in the case of how the EU's General Data Protection Regulation (GDPR) is reshaping contractual provisions and incentivizing the development of codes of conduct.[51] However, one reform that does have the potential for substantially bending the curve on software resilience is products liability, which is the topic we turn to next.

A. Products Liability: Origins, Evolution, & Application to Software

One might imagine a legal order in which the sole liability for poorly performing products or services was breach of an express contract, criminal accountability for causing death or injury, or tort liability for committing fraud or a trespass. This appears to have once been the common law of real property leases: "[T]here is no contract, still less a condition, implied by law on the demise of real property only, that it is fit for the purpose for which it is let."[52] Such a rule imposed a sort of

50. *See* Janine Hiller, Kathryn Kisska-Schulze & Scott Shackelford, *Cybersecurity Carrots and Sticks*, 61 AM. BUS. L.J. 5, 18–22 (2024).

51. *See, e.g.*, General Data Protection Regulation, art. 40, 2016 O.J. (L 119), https://gdpr-info.eu/art-40-gdpr/ [https://perma.cc/555F-4BGZ].

52. Hart v. Windsor, (1843) 12 M. & W. 68, 87–88 (Eng.); *see also* Southwark London

obligation of due diligence on the lessee of property in accordance with the maxim *caveat emptor* or "let the buyer beware."[53]

In contracts for the sale of goods, however, the common law has imposed a duty to provide a salable good to a purchaser with no opportunity to inspect it.[54] This rule has the arguable merits of dispensing with *caveat emptor* when the buyer is disabled by distance or inaccessibility from examining the goods, while preserving *caveat emptor* where the buyer can prevent a failed deal by inspection and guaranteeing freedom of contract as to second-hand or repairable goods while minimizing litigation. One author describes the doctrine concerning the sale of machines (as of about 1920) as operating in such a way.[55] Like the economic loss doctrine described below, a loose warranty of salable goods, set at a low level, permits a diversity of products to be marketed across a wide price-quality spectrum.

A further warranty that might be implied is fitness for the particular purpose of the buyer underlying the sale, and fitness for the typical or intended use of the good.[56]

Borough Council v. Mills, [1999] 4 All ER 449, 449–53 (quoting Edler v. Auerbach, (1950) 1 K.B. 359, 374 (Eng.) ("'It is the business of the tenant, if he does not protect himself by an express warranty, to satisfy himself that the premises are fit for the purpose for which he wants to use them . . . .'")). There may be non-contractual statutory duties to ensure the habitability of short-term residential property leased to the public and to repair the structure and fixtures of a leased dwelling. *See* PETER SPARKES, A NEW LANDLORD AND TENANT 243–60 (2001). Some duties cover "defects," as in a manufacturing defect that should be known to a seller. Kellogg Bridge Co. v. Hamilton, 110 U.S. 108, 115–16 (1884).

53. *See* WILLIAM W. STORY, A TREATISE ON THE LAW OF SALES OF PERSONAL PROPERTY, WITH ILLUSTRATIONS FROM THE FOREIGN LAW., 313, 315, 317 (1847). The civil law was said to have rejected *caveat emptor* in favor of *caveat venditor*. *See* Hargous v. Stone, 5 N.Y. 73, 84 (1851); 1 JERRY J. PHILLIPS & ROBERT E. PRYOR, PRODUCTS LIABILITY 47 (2d ed. 1993) (under the influential French Civil or "Napoleonic Code," "Caveat venditor, with a theory of implied warranty . . . had always been part of [the] law.").

54. *See, e.g.*, English v. Spokane Comm'n Co., 57 F. 451, 455 (6th Cir. 1894); Murchie v. Cornell, 155 Mass. 60, 60 (1891) (citing, inter alia, Jones v. Just, [1868] L.R. 3 Q.B. 197, 37 L.J.Q.B. 89 (Eng.)); Gardiner v. Gray, (1815) 4 Camp. R. 144, 171 Eng. Rep. 46); William L. Prosser, *The Implied Warranty of Merchantable Quality*, 21 CAN. BAR REV. 446, 456 n.60 (1943); STORY, *supra* note 53, at 315; 3 SAMUEL WILLISTON, THE LAW OF CONTRACTS 2769 (1920). A like rule applies to the implied warranty of good title to the goods, like salability implied by the fact of offering them for sale; liability here was strict, not avoided by good faith. *See* Allen v. Hammond, 36 U.S. 63, 63, 72 (1837) (mentioning sale of a dead horse as precedent for denying recovery to claimant to contract to find a ship); Coolidge v. Brigham, 42 Mass (1 Met.) 547, 551 (Mass. 1840); STORY, *supra* note 53, at 313–14; Charles Henry Tuttle, *Money Paid Under Mistake as to a Collateral Fact*, 63 ALBANY L.J. 340, 349 (1901).

55. *See* A.F. HARSHBARGER, THE MANUFACTURER'S WARRANTY 10–11 (1921) ("Manufacturers of machinery are generally held to an implied warranty that their machines are reasonably fit for the purpose for which they were purchased, but their warranty like that of the manufacturer generally does not extend to particular uses to which the buyer may put them. It extends to the general uses, and does not warrant more than that the machine is suitable for those uses, not even as suitable as other machines in the same class may be."). Williston implies that a machine which does not work and is unmerchantable might be the subject of a "mutual mistake" justifying rescission. WILLISTON, *supra* note 54, at 2769.

56. *See, e.g.*, *Kellogg Bridge Co.*, 110 U.S. at 115 (citing Leopold v. Vankirk, 27 Wis. 152 (1870)); STORY, *supra* note 53, at 317; *cf.* LAWRENCE M. FRIEDMAN, A HISTORY OF

The buyer is once again vulnerable and may be frustrated in protecting himself or herself between the contract's execution and delivery of the goods.[57] For similar reasons, variation of a delivered good from a manufacturer's model or sample would breach an implied warranty.[58] As applied to artisans and mechanics, this rule could take on the spirit of a malpractice regime and recognize the negligence principle that measures a duty of care by training, ability, marketplace norms, and overall reasonableness.[59] By the nineteenth century, this warranty applied "even to latent defects undiscoverable by the seller."[60]

Under U.S. federal law, there are overlapping and cross-cutting consumer protections. For example, the Magnuson-Moss Warranty Act permits a consumer to allege one of several things with respect to a dangerous or ineffective product: a violation of specific federal protections, a breach of an express warranty or service contract under state law, or breach of an implied state-law warranty.[61]

At common law, negligence, strict liability, unjust enrichment, misrepresentation, and breach of the implied duty of good faith and fair dealing, as well as promissory estoppel, tortious interference with contract, emotional distress, unfair competition and privacy claims, and breach of contract are relevant in products liability cases.[62]

AMERICAN LAW 521 (4th ed. 2019) ("[I]mplied warranties almost nullified the rule of *caveat emptor*.").

57. *See, e.g.*, Heath Dry Gas Co. v. Hurd, 193 N.Y. 255, 255 (1908); Queens City Glass Co. v. Pittsburgh Clay Pot Co., 55 A. 447, 449 (1903); STORY, *supra* note 53, at 317–18; *cf.* FRANCIS B. TIFFANY, HANDBOOK OF THE LAW OF SALES 171–72 (1895).

58. *See, e.g.*, William Anson Wood Mower & Reaper Co. v. Thayer, 3 N.Y.S. 465, 467 (Gen. Term. 1888); Ideal Wrench Co. v. Garvin Mach. Co., 72 N.Y.S. 662, 664 (App. Div. 1901).

59. *See, e.g.*, Eberle v. Hughes, 909 N.Y.S.2d 273 (App. Div. 2010); STORY, *supra* note 53, at 318; Note, *The Liability of the Manufacturer of a Defective Automobile to a Sub-Vendee*, 29 HARV. L. REV. 866, 866 (1916). According to one case:

> Although the policy of the law has not imposed on the towing boat the obligation resting on a common carrier, it does require on the part of the persons engaged in her management, the exercise of reasonable care, caution, and maritime skill, and if these are neglected, and disaster occurs, the towing boat must be visited with the consequences.

The Steamer Syracuse, 79 U.S. 167, 171 (1870); *cf.* Coggs v. Bernard (1703) 92 Eng. Rep. 107; 2 Ld. Raym. 909 (Eng.); Moneypenny v. Hartland (1824) 1 C.& P. 351 (Eng.); Shiells v. Blackburne (1789) 1 H. Bl. 159 (Eng.).

60. TIFFANY, *supra* note 57, at 172 n.101. *But see id.* at 171 n.96, 172 n.101 (citing Hoe v. Sanborn, 21 N.Y. 552 (1860)); Bragg v. Morrill, 49 Vt. 43 (1876); Hargous v. Stone, 5 N.Y. 73, 88 (1851); Rollis Engine Co. v. Eastern Forge Co., 59 A. 382, 382 (N.H. 1904); 6 ARTHUR LINTON CORBIN, CORBIN ON CONTRACTS 186 (2002).

61. *See, e.g.*, Schimmer v. Jaguar Cars, Inc., 384 F.3d 402, 405 (7th Cir. 2004); MacKenzie v. Chrysler Corp., 607 F.2d 1162, 1166 n.7 (5th Cir. 1979); Magnuson Moss Warranty—Federal Trade Commission Improvement Act of 1975, 15 U.S.C. § 2301; AM. JUR. 2d *Consumer Product Warranty Acts* §§ 1–50; 93 N.Y. JUR. 2D. *Sales and Exchanges of Personal Property* § Summary.

62. *See*, *e.g.*, Quinteros v. Innogames, No. 22-35333, 2024 WL 132241 (9th Cir. Jan. 8, 2024); *In re* Social Media Adolescent Addiction/Personal Injury Prod. Liab. Litig., No. 4: 22-

There are subtle distinctions between design defect cases, duty to warn cases sounding in negligence, strict products liability involving a failure or failures to warn consumers, and breach of implied warranty cases.[63] In a design defect claim theorized as negligence, a central question will be whether the design, making, installation, repair, or other provision of a product was negligent, meaning that it fell below, for example, "industry standards."[64] In a strict products liability design defect claim, a slightly different question could be triable: whether a product did not perform as "safely" as a "[reasonable] consumer would have expected," even if said consumer "misused" the product in a "reasonably foreseeable way."[65] A negligence case may involve balancing "the likelihood and severity of potential harm from the product," harm which the designer or maker should have known or did know about, against "the burden of taking safety measures to reduce or avoid the harm."[66]

Challenges to the design of software, online platforms, and AI systems using products liability theories have been in the news in recent years. An initial question is whether, being unlike traditional tangible goods, certain programs, tools, networks, or models are not "products." The content of books, films, certain video games, formulas, algorithms, recommendations, and other expressive works have evaded treatment as products at times.[67] Some scholars have proposed that products

---

md-03047-YGR, 2023 WL 7524912 (N.D. Cal. Nov. 14, 2023), *mot. to certify interlocutory appeal denied*, 2024 WL 1205486 (N.D. Cal. Feb. 2, 2024); Sasso v. Tesla, Inc., 584 F. Supp. 3d 60 (E.D.N.C. 2022); Moore v. Apple, Inc., 73 F. Supp. 3d 1191, 1202–05 (N.D. Cal. 2014); Opperman v. Path, Inc., 87 F. Supp. 3d 1018, 1029–55 (N.D. Cal. 2014); *cf.* Herrick v. Grindr LLC, 765 F. App'x 586, 591 (2d Cir. 2019).

63. *See, e.g.*, Judicial Council of California Civil Jury Instructions §§ 1201–05, 1220–23 (2024).

64. *See id.* §§ 1220–21.

65. *Id.* § 1203.

66. *Id.* § 1221; *cf.* Lemmon v. Snap, Inc., 995 F.3d 1085, 1086 (9th Cir. 2021) (treating social-media app as negligently designed does not impermissibly treat it as the publisher or speaker of information provided by a user in contravention of 47 U.S.C. § 230).

67. *See, e.g.*, Rodgers v. Christie, 795 F. App'x 878, 879–80 (3d Cir. 2020) (algorithm or formula not like a tangible product); James v. Meow Media, Inc., 300 F.3d 683, 701 (6th Cir. 2002) (film or video game not like a tangible product); Estate of B.H. v. Netflix, Inc., No. 4-21-cv-06561-YGR, 2022 WL 551701, at *1 (N.D. Cal. Jan. 12, 2022) (streaming series not like a tangible product), *aff'd on other grounds*, No. 22-15260, 2024 WL 808797 (9th Cir. Feb. 27, 2024); Gorran v. Atkins Nutritionals, Inc., 464 F. Supp. 2d 315, 319, 323–29 (S.D.N.Y. 2006) (citing Winter v. G.P. Putnam's Sons, 938 F.2d 1033, 1034 (9th Cir. 1991)) (diet program not like a tangible product); Jones v. J.B. Lippincott Co., 694 F. Supp. 1216, 1217 (D. Md. 1988); Walter v. Bauer, 439 N.Y.S.2d 821, 822–23 (Sup. Ct., 1981); RESTATEMENT (THIRD) OF TORTS § 19(a) (AM L. INST. 1998). *But see In re* Social Media Adolescent Addiction/Personal Injury Prod. Liab. Litig., 702 F. Supp. 3d 809, 840–42 (N.D. Cal. 2023) (citing, inter alia, Lemmon v. Snap, Inc., 995 F.3d 1085, 1092 (9th Cir. 2021)) (distinguishing social media platforms' design features from films or streaming series and analogizing them to ride-sharing apps); AM v. Omegle.com, LLC, 614 F. Supp. 3d 814, 817 (D. Or. 2022); Brookes v. Lyft, Inc., 2022 WL 19799628, at *3 (Fla. Cir. Ct. Sept. 30, 2022). *See generally* Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425, 466 (2008); Frances E. Zollers, Andrew McMullin, Sandra N. Hurd & Peter Shears, *No More Soft Landings for Software: Liability for Defects in an Industry That Has Come of Age*, 21 SANTA CLARA COMPUT. & HIGH TECH. L.J., 745, 759–

liability principles should be applied to discriminatory or harmful algorithms or platform design policies.[68]

Theoretically, some of the reasons for imposing liability on designers, manufacturers, lessors, suppliers, repair persons, and others involved in product provision may apply to dangerous, ineffective, unsalable, or inadequately updated software, platforms, or AI. One such reason is known as loss spreading, which spreads the risk of new experiments and dangerous enterprises beyond the occasional unlucky victim of their accidents.[69] A rival to loss spreading as a justification of products liability law is economic efficiency, which calls for deterrents to inefficient business practices.[70] One economic phenomenon or trend relevant to both loss spreading and deterrence is the concept of the lowest cost avoider or least cost avoider: Why compel a consumer or user to personally bear the full cost of a practice that could be much more cheaply prevented by a big company?[71] Another concept or label that can be important is information asymmetry, which concedes the vulnerability and relative ignorance of the consumer, even a business customer, as compared with a designer, manufacturer, or vendor.[72] While such concepts (relating to cost of prevention or access to information) do not automatically weigh in favor

---

60 (2005).

68. *See, e.g.*, Kevin Ofchus, *Cracking the Shield: CDA Section 230, Algorithms, and Product Liability*, 46 U. ARK. LITTLE ROCK L. REV. 27 (2023); Allison Zakon, Comment, *Optimized for Addiction: Extending Product Liability Concepts to Defectively Designed Social Media Algorithms and Overcoming the Communications Decency Act*, 2020 WIS. L. REV. 1107; *cf. In re Social Media Adolescent Addiction*, 702 F. Supp. 3d at 837–60; Adam Candeub, *Reading Section 230 as Written*, 1 J. FREE SPEECH L. 139 (2021); Danielle Keats Citron, *How to Fix Section 230*, 103 B.U. L. REV. 713 (2023).

69. *See* Greenman v. Yuba Power Prod., Inc., 377 P.2d 879, 901 (Cal. 1963) (citing Escola v. Coca Cola Bottling Co., 150 P.2d 436 (Cal. 1944) (Traynor, J., concurring)); *see also* Chavez v. S. Pac. Transp. Co., 413 F. Supp. 1203, 1207–08 (E.D. Cal. 1976); WILLIAM L. PROSSER, HANDBOOK OF THE LAW OF TORTS 318 (2d ed. 1955).

70. *See, e.g.*, Hall v. E.I. Du Pont De Nemours & Co., Inc., 345 F. Supp. 353, 368 (E.D.N.Y. 1972) ("A rigorous rule of liability with enhanced possibilities of large recoveries is an 'incentive' to maximize safe design or a 'deterrence' to dangerous design, manufacture, and distribution." (citing, inter alia, Vandermark v. Ford Motor Co., 391 P.2d 168, 170–72 (1964))).

71. *See, e.g.*, Beauchamp v. Russell, 547 F. Supp. 1191, 1197 (N.D. Ga. 1982) ("The responsibility for information collection and dissemination should rest on the party who has the greatest access to the information and who can make it available at the lowest cost." (citing Comment, *Apportionment Between Partmakers and Assemblers in Strict Liability*, 49 U. CHI. L. REV. 544 (1982))); *see also* Ins. Co. N. Am. v. Forty-Eight Insulations, Inc., 633 F.2d 1212, 1231 (6th Cir. 1980) (Merritt, J., dissenting) (advocating a legal rule that "better spreads losses that the parties claim were unforeseen by the industry as a whole" and "tends to reduce the costs of future accidents by placing the burden of liability on insurers [who are] best able to evaluate the risks of hazardous activity and best able to deter or minimize the ultimate tort costs of that activity" because "accident costs [are] minimized by placing ultimate liability on 'least cost avoider'" (quoting GUIDO CALABRESI, THE COST OF ACCIDENTS (1971))).

72. *See* Anthony M. Marino, *Market Share Liability and Economic Efficiency*, 57 S. ECON. J. 667 (1991); Andreas Loukakis, *Product Liability Ramifications for Damage Caused by Erroneous GNSS Signals*, *in* DISPUTE SETTLEMENT IN THE AREA OF SPACE COMMUNICATION 175–200 (Mahulena Hofmann ed., 2015).

of extended liability, they can be leveraged into advocacy for extended liability.[73] One potentially multi-trillion dollar question is determining how these legal remedies may apply in practice, such as in cases such as the 2024 CrowdStrike incident. That incident is unpacked next, and we return to the issue of products liability in the comparative case studies included in Part III.

B. Software Updates Accountability: CrowdStrike Case Study

All software contains mistakes, commonly referred to as "bugs."[74] These bugs arise due to the inherent complexity of software development where even minor errors can lead to significant consequences.[75] For example, poor software quality costs U.S. organizations approximately $2.84 trillion, according to a 2018 report by the Consortium for IT Software Quality (CISQ).[76] Some of these bugs are "exploitable," meaning that someone who is aware of the mistake can use it to gain unauthorized control over the software without needing alternative means to access the device. Other bugs are non-exploitable, requiring a malicious actor to first gain access to the software or device through other means before leveraging the bug to escalate their control.[77] Attackers often exploit multiple bugs within complex systems or networks to achieve their objectives. Further, some bugs are mere errors that do not introduce any vulnerability and cannot be used by attackers to compromise a system. While all vulnerabilities are bugs, not all bugs are

---

73. *Cf.* Marino, *supra* note 72, at 667 (arguing that one driver of the trend toward increasing—or even strict—products liability is that consumers lack adequate information).

74. See, for example, Steve McConnell, CODE COMPLETE: A PRACTICAL HANDBOOK OF SOFTWARE CONSTRUCTION ch. 22 (2d ed. 2004), where the author outlines that there are between one and twenty-five bugs per thousand lines of deployed code on average. This average is constant across major programming languages and is not influenced by the nature of the software. The etymology of the word "bug" is somewhat contested. The term is often falsely attributed to Grace Hopper, who recalled a moth interfering with a punch card. However, this is more accurately described as the first time that the term "bug" was used in the context of a computer error. *See generally What Happened on September 9th*, COMPUT. HIST. MUSEUM, https://www.computerhistory.org/tdih/september/9/#:~:text=On%20September%209%2C%201947%2C%20a,members%20wrote%20in%20the%20log [https://perma.cc/Z4EG-D5NZ]. Thomas Edison had already used the term "bug" in the 1830s as a synonym for "little faults" in his letter to Tivadar Puskás. THOMAS PARK HUGHES, AMERICAN GENESIS: A CENTURY OF INVENTION AND TECHNOLOGICAL ENTHUSIASM, 1870-1970 75 (1989).

75. See, for example, Alana Maurushat & Kathy Nguyen, *The Legal Obligation to Provide Timely Security Patching and Automatic Updates*, 3 INT'L CYBERSECURITY L. REV. 437 (2022), which provides multiple examples of vulnerabilities being exploited to compromise systems.

76. Herb Krasner, *The Cost of Poor Quality Software in the US: A 2018 Report*, CONSORTIUM FOR IT SOFTWARE QUALITY 5 (Sept. 26, 2018), https://www.it-cisq.org/the-cost-of-poor-quality-software-in-the-us-a-2018-report/ [https://perma.cc/E2MX-X45K].

77. See, for example, Iain Nash, *Cybersecurity in a Post-Data Environment: Considerations on the Regulation of Code and the Role of Producer and Consumer Liability in Smart Devices*, COMPUT. L. & SEC. REV., APR. 2021, at 1, 5, which discusses the nature of vulnerabilities in more detail.

vulnerabilities. Bugs are flaws or errors in software code that may affect functionality or performance. Vulnerabilities are a subset of bugs that can be exploited by attackers to gain unauthorized access or cause harm.

Given that all software contains bugs, what options are available to software developers to reduce their impact? In essence, developers can either ignore the errors, hoping they are not exploited, or they can make changes to the code to remove the errors. These changes are known as "patches."[78] Patches are updates to the software that remove the bug and ideally replace it with error-free code. However, since patches are changes to the codebase, they introduce their own set of potentially new vulnerabilities through bugs and/or changes in how the software operates as seen in the 2024 CrowdStrike update discussed below. In simple applications, these changes may not pose significant issues. However, in complex systems, a change can lead to alterations in how the software operates, potentially causing other dependent software applications to fail in the interconnected ecosystem.[79]

This problem is further exacerbated by the fact that software developers also issue updates to improve or add functionality to their software. Unlike patches, these "feature updates" are not developed to remediate security issues, but rather to introduce new features or optimize performance. Both patches and feature updates are types of software updates, but they serve different purposes. Software updates, regardless of their nature, also present a tension. On one hand, developers aim for users or administrators to deploy updates promptly. On the other hand, users or administrators may be concerned that updates could degrade the application, network, or system, leading them to delay deployment. For example, it takes organizations an average of 171 days to remediate 50% of the security vulnerabilities found in their applications, increasing the window of opportunity for attackers, according to a report by Veracode.[80] In this sense, when developers choose to release an update, they face an additional choice: They can either release the patch and wait for the user or administrator to deploy it, or they can embed a mechanism in the software that allows them to deploy the patch automatically.

A recent incident involving CrowdStrike, a leading cybersecurity firm, provides an illustrative example of the complex interplay between automatic software updates, system stability, and vendor liability within the context of the legal system that technology operates under. CrowdStrike provides endpoint security solutions through its Falcon platform, which is deployed on clients' devices to detect and prevent cyber threats. In this incident, CrowdStrike automatically deployed an update to their Falcon sensor that contained a bug with materially negative effects on users' systems,[81] although it did not introduce a new vulnerability. According to

---

78. *See, e.g.*, *Understanding Patches and Software Updates*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Feb. 23, 2023), https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates [https://perma.cc/2AMM-RLKV].

79. *See generally* SCOTT J. SHACKELFORD, THE INTERNET OF THINGS: WHAT EVERYONE NEEDS TO KNOW (2020) (exploring the security, privacy, and governance challenges in the IoT context).

80. *2025 State of Software Security: A New View of Maturity*, VERACODE 6 (2025), https://www.veracode.com/wp-content/uploads/2025/02/State-of-Software-Security-2025.pdf [https://perma.cc/EWS7-Z36Y].

81. Sean Michael Kerner, *CrowdStrike Outage Explained: What Caused It and What's*

internal incident reports, the update included an incorrectly formatted configuration file that caused systems running Windows operating systems to fail during startup.[82]

The problematic update was pushed directly to customers' devices without requiring any input or consent from users or system administrators. This automatic deployment capability is designed to ensure that clients receive timely updates to protect against emerging threats. However, the incident raises significant questions about the balance between the necessity of prompt security updates and the potential risks to system stability posed by insufficiently tested updates. In fact, third-party software applications are now key to the successful operation of the operating system. For instance, the update here was a file read and processed during the startup sequence of the Windows operating system. The failure of the update meant that the operating system itself could not start. Although the update originated from CrowdStrike (not Microsoft), it functioned as an update to Windows because once deployed, CrowdStrike's application became part of the Windows kernel.[83] This demonstrates how bugs in third-party software can have a direct and detrimental impact on the operating system and other software applications.

From a technical standpoint, the incident illustrates the risks associated with automatic updates, especially when the software operates at a fundamental level within the system architecture. While automatic updates can rapidly protect devices against new threats, they can also introduce significant risks if not thoroughly tested. The fact that the update caused system-wide failures highlights the potential for such updates to do more harm than good if proper quality assurance processes are not followed. The risk is exacerbated by the fact that software vendors, like CrowdStrike, commonly include clauses in their contracts that limit their liability for damages resulting from software errors, including those introduced through updates. These limitations of liability and warranty disclaimers are standard in the software industry and are often enforced through End User License Agreements (EULAs) or service contracts.

A review of CrowdStrike's standard contract terms reveals provisions that significantly limit the company's liability. For instance, their agreements may include language that:

- Disclaims all warranties, express or implied, including warranties of merchantability and fitness for a particular purpose.
- Limits the vendor's liability to a refund of fees paid or a nominal amount, regardless of the nature of the claim.
- Excludes liability for indirect, incidental, consequential, or punitive damages.[84]

Next, TECHTARGET (Oct. 29, 2024), https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next [https://perma.cc/WY66-P26M].

82. *Executive Summary: CrowdStrike Preliminary Post Incident Review (PIR): Content Configuration Update Impacting the Falcon Sensor and the Windows Operating System (BSOD)*, CROWDSTRIKE (2024), https://www.crowdstrike.com/wp-content/uploads/2024/07/CrowdStrike-PIR-Executive-Summary.pdf [https://perma.cc/RH6A-NX7Z].

83. Kerner, *supra* note 81.

84. *CrowdStrike Terms and Conditions*, CROWDSTRIKE, https://www.crowdstrike.com/en-us/terms-conditions/ [https://perma.cc/W7V2-2MC9].

Such clauses can severely restrict the recourse available to customers when automatic updates cause system failures or other significant disruptions. In the case of the CrowdStrike incident, affected organizations may find that their ability to recover damages is limited by these contractual provisions. However, the enforceability of liability limitations is not absolute. Courts may scrutinize these clauses, particularly if they result in unconscionable outcomes or if the vendor's negligence leads to substantial harm. In jurisdictions with consumer protection laws, limitations on liability may be deemed unenforceable if they are considered unfair or if they violate statutory protections.[85] Furthermore, the CrowdStrike incident raises a direct challenge for policymakers, who in various jurisdictions have begun to require software developers to deploy security updates to their code bases. This challenge is discussed further in the next Section.

C. Automatic Updates and Their Security Challenges

Microsoft Windows XP was one of the earliest operating systems capable of automatically checking for and deploying security updates.[86] Microsoft's patch schedule involves releasing security updates on the second Tuesday of every month, known as "Patch Tuesday," at 10:00 AM Pacific Standard Time.[87] This practice was formalized in 2003, as mentioned in the introduction, replacing the previous "ship when ready" approach to provide a more predictable and manageable update process for system administrators.[88] Administrators could test updates in controlled environments before rolling them out to all users, mitigating the risk of updates causing unforeseen issues. Over time, however, Windows has shifted toward a model where updates—both security patches and feature updates—are deployed automatically with minimal user involvement. They are released on the second Tuesday of every month (the "B" Release/Patch Tuesday), and feature updates are released on the third and fourth Tuesdays of each month (the "C" and "D" releases).[89] This change aims to enhance security by ensuring that critical updates are applied promptly across all systems. Urgent security patches, however, can be released out-of-cycle when immediate attention is required.[90]

---

85. *See, e.g.*, *Legal Implications of the Crowdstrike Incident: A Wake-up Call for IT Security*, UNYER GLOB. ADVISORS (Aug. 8, 2024), https://www.unyer.com/legal-implications-of-the-crowdstrike-incident-a-wake-up-call-for-it-security/ [https://perma.cc/34SJ-FKRG].

86. *See* Bjoern M. Luettmann & Adam C. Bender, *Man-in-the-Middle Attacks on Auto-Updating Software*, 12 BELL LABS TECH. J. 131, 134 (2007).

87. *See, e.g.*, *Security Update Guide FAQs*, MICROSOFT, https://www.microsoft.com/en-us/msrc/faqs-security-update-guide/ [https://perma.cc/VEN2-WKBV].

88. *See* Reguly, *supra* note 2.

89. *See, e.g.*, John Wilcox, *Windows 10 Update Servicing Cadence*, MICROSOFT: WINDOWS IT PRO BLOG (Aug. 1, 2018), https://techcommunity.microsoft.com/t5/windows-it-pro-blog/windows-10-update-servicing-cadence/ba-p/222376 [https://perma.cc/A9AD-EQ8F].

90. Shayan Naveed, *Software Patches: 7 Types of Patches to Remember*, PUREVERSITY (May 27, 2024), https://www.pureversity.com/blog/types-of-patches [https://perma.cc/8XW6-GNKU].

While it remains possible to disable Windows updates, doing so is not straightforward and requires altering core system settings or modifying Windows services, which is beyond the expertise of the average user.[91] In fact, the scheduled release process was developed with the expectation that system administrators would be involved in the deployment of patches.[92] The transition away from system administrators to the end-user reflects Microsoft's prioritization of the widespread adoption of updates to protect users from emerging threats.[93] In contrast, Apple's macOS comes with automatic operating system updates turned on by default, but users can easily disable this feature through system preferences.

Linux operating systems, which are predominantly used on servers and managed by professionals or enthusiasts, typically do not have automatic updates enabled by default. Instead, they offer an opt-in mechanism that allows administrators to enable automatic updates for security patches, feature updates, or all types of updates, depending on their needs. This approach provides greater flexibility and control, which is essential in environments where stability and compatibility are critical. Yet it can also give rise to significant security oversights, such as in the case of the infamous Equifax breach.[94]

The incident is a pertinent example of the ongoing challenges in the cybersecurity industry, especially related to supply chain risk in the digital infrastructure. In fact, Desai and Makridis point out that the professional services sector generates more cyber vulnerabilities than the traditionally classified "critical infrastructure sectors" precisely because of supply chain linkages.[95] We discuss this further in the next Section. This breach underscores the arguments made in the 2023 U.S. National

---

91. *See* Makenzie Buenning, *4 Ways to Easily Disable Windows Updates*, NINJAONE, https://www.ninjaone.com/blog/4-ways-to-disable-windows-updates/ (Jan. 21, 2025) [https://perma.cc/T5BL-53Q9].

92. *See* Christopher Budd, *Ten Years of Patch Tuesdays: Why It's Time to Move On*, GEEKWIRE (Oct. 31, 2013, 3:03 PM), https://www.geekwire.com/2013/ten-years-patch-tuesdays-time-move/ [https://perma.cc/N7KA-CYYV] (summarizing a discussion by a former member of the Microsoft Team who was part of the development of "Patch Tuesday" and who references how it was developed to reduce the load on system administrators).

93. The choice given to users is "deploy now" or "deploy later." *See The Importance of Computer Software Updates & Security Patches*, MICROSOFT (July 14, 2022), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/computer-software-update [https://perma.cc/BD25-63G6] (outlining why auto updates are needed); *The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack*, MICROSOFT (May 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/ [https://perma.cc/8CKZ-P32S] (outlining the effect of automatic updates on the collective good).

94. *See* Steven Vaughan-Nichols, *Equifax Blames Open-Source Software for Its Record-breaking Security Breach: Report*, ZDNET (Sept. 11, 2017), https://www.zdnet.com/article/equifax-blames-open-source-software-for-its-record-breaking-security-breach/ [https://perma.cc/5G7M-R7S8].

95. Deven R. Desai & Christos A. Makridis, *Identifying Critical Infrastructure in a World with Supply Chain and Cross-Sectoral Cybersecurity Risk*, 62 JURIMETRICS J. L. SCI. & TECH. 173, 182, 193 (2022).

Cybersecurity Strategy, which calls for greater accountability and potential liability for technology providers when their products fail to protect against security threats.

The updated frameworks put in place by Microsoft, Apple, or the various maintainers of Linux distributions are not the result of any legal requirements in any jurisdiction. Indeed, at the time of writing, there is little in the way of legislative requirements, or guidance, when it comes to software updates. Within the European Union, the Cyber Resilience Act (CRA) requires that developers continue to develop security updates and make these available to users for at least five years or for the expected life cycle of the product. The CRA also states, in the non-binding recitals, that security updates should be delivered separately from functionality updates and that users should not be required to adopt new functionality to receive security updates.[96] The topic is discussed further in Part III.

When it comes to the question of automatic updates, however, the CRA is less prescriptive. While the CRA recommends the use of automatic updates, it does not require them.[97] This has quite profound liability consequences, as software that contains a vulnerability, and for which a patch has been developed, can be considered as in conformity with the CRA even though the patch was not deployed.[98]

Outside of the CRA, there are two European Directives[99]—the Sale of Goods Directive and the Digital Content Directive—that reference security updates, as well as a European Directive relating to the green transition.[100] These directives require

---

96. Position of the European Parliament adopted at first reading on March 12, 2024, with a view to the adoption of Regulation (EU) 2024/1868 of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Council Regulations 168/2013, 2013 O.J. (L 60/52) and Council Regulation 2019/1020, 2019 O.J. (L 169/1) and Directive (EU) 2020/1828, 2020 O.J. (L 409) Recital 55 (Cyber Resilience Act).

97. *See id.* at Annex 1, Part 1(1)(c). The use of the phrase "where applicable" returns the choice of whether to use automatic updates or require the user to deploy updates manually to the software developer.

98. *See* CRA, art. 13(9) ("Manufacturers shall ensure that each security update . . . which has been made available to users during the support period, remains available after it has been issued for a minimum of 10 years or for the remainder of the support period, whichever is longer."); *cf.* CRA, Recital 56 (indicating that users should be able to opt out of automatic updates, by deactivating them, although a "manufacturer should inform users about vulnerabilities and make security updates available without delay").

99. Directive 2019/770, of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services, 2019 O.J. (L 136) 1; Directive 2019/771 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Sale of Goods, Amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, 2019 O.J. (L 136) 28 (EU); Regulation 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), 2024 O.J. (L 2847) 11.

100. Directive 2024/825 of the European Parliament and of the Council of 28 February 2024 Amending Directives 2005/29/EC and 2011/83/EU as Regards Empowering Consumers for the Green Transition Through Better Protection Against Unfair Practices and Through Better Information 2024, 2024 O.J. (L 6) 3.

that digital goods and services meet certain conformity criteria, which include providing necessary updates to keep products in compliance with the contract of sale. However, these references are relatively general and do not prescribe specific update mechanisms or schedules. The choice of how updates are to be deployed, with the subsequent conformity and liability consequences, is left to the software developer.

In other jurisdictions, such as the United States, there is currently no federal legislation mandating how software updates should be managed or deployed. The States of California and Oregon have, however, introduced legislation that imposes cybersecurity requirements on the developers of embedded software.[101] Both pieces of legislation require "reasonable security," and it is hard to conclude that "reasonable" efforts do not include security updates,[102] although once again, the choice of how security updates once developed are deployed, would seem to be left to the developer.

In the United Kingdom, the 2022 Product Security and Telecommunications Infrastructure Act also imposes cybersecurity requirements on the developers of embedded software, requiring them to state a support period and provide security updates during that time.[103] However, there is no discussion as to what form the update mechanism should be, only that there is one.

The consequences for a policymaker with regard to automatic updates are severe. If software contains an exploitable bug, the fastest way for that bug to be remedied is through the automatic deployment of a patch. Allowing the user to choose when, if ever, to deploy a security update can allow an exploitable bug to persist. Furthermore, if an exploitable bug is present in a product in which the user does not interact with the software directly, such as an Internet of Things (IoT) device, the user may not be aware of the security updates. The alternative is to require that updates are automatic, either immediately or within a pre-defined window. However, the CrowdStrike update is an example of the risks that can arise with automatic updates, especially when they are deployed to all users immediately. Therefore, it is clear how there is a tension between automaticity of updates and system resilience.

While it is positive that policy has begun to move toward recognizing that security updates exist and are required over the lifetime of software-based products, the actual practice of updating software has not been engaged with by policymakers. Indeed, software developers are now facing certain jurisdictional requirements where they will be required to make software updates available and encouraged to deploy them quickly. However, they are not provided with any safe harbors in terms of specific update management and will be held responsible for harm incurred by certain classes of users if these updates have negative impacts. Such a scenario could

---

101. In 2018, Title 1.81.26. Security of Connected Devices 2018, CAL. CIV. CODE § 1798.91.04 (West 2023), was passed, which was followed in 2019 by Security requirements for Internet-connected devices, OR. REV. STAT. § 646A.813 (2019).

102. CAL. CIV. CODE § 1798.91.04 (West 2023); OR. REV. STAT. § 646A.813(2) (2019); *see, e.g.*, Shackelford et al., *supra* note 14, at 102–03.

103. Product Security and Telecommunications Infrastructure Act 2022, c. 46, § 3 (UK).

include the rapid rectification of a major exploitable bug, but at the cost of introducing some other, perhaps non-exploitable bug.[104]

One additional concept for policymakers to clarify in legislation is the differentiation between security patches and feature updates. However, updates are complicated by the recent developments in the AI field. In the case of advanced AI, the differentiation between a patch and a feature update is less clear.[105] If a new threat is detected, updates that enable detection of this new threat may require interaction with the kernel in a new way, which both increases the functionality of the program and is a response to a security threat. Essentially, patches may also become feature updates. It is unclear whether this was the case in the CrowdStrike example, but it demonstrates how some security patches will require feature and core level changes to work as designed, including in the critical infrastructure context.

D. Application to Critical Infrastructure Protection

The U.S. Department of Homeland Security (DHS) has traditionally followed a static classification of sixteen critical infrastructure sectors, though new applications, such as election systems, have been added over time.[106] Software is replete across these sectors as they have become increasingly "smart" over the years, with electric utilities being a case in point given the drive for increased resilience and distribution in the face of climate change.[107] This interconnection has also bred insecurity, though, with an increasing number of cyberattacks launched by a wide range of nation-state and non-state groups impacting the grid, with the war in Ukraine being a case in point.[108] Water utilities have also been targeted, along with natural gas pipelines, healthcare organizations, and other critical sectors in the United States and around the world. Thus far, effective collective action to address the situation has proven elusive. The dependence on software, combined with the mounting technical debt of outdated systems along with the expanding attack surface from many more devices and systems being connected to the internet, highlights the stakes of improving software resilience and accountability across critical infrastructure sectors.[109]

---

104. *See, e.g.*, Iain Nash, DeBrae Kennedy-Mayo, Peter Swire & Annie Antón, *Legal Issues in Reconciling Data Protection, AI, and Cybersecurity Under EU Law*, 89 MO. L. REV. 871 (2024).

105. *See* Scott J. Shackelford, Bruce Schnier, Michael Sulmeyer, Anne Boustead, Ben Buchanan, Amanda N. Craig Deckard, Trey Herr & Jessica Malekos Smith, *Making Democracy Harder to Hack*, 50 U. MICH. J.L. REFORM 629 (2017); *see, e.g.*, Nash, *supra* note 104.

106. *See* Shackelford et al., *supra* note 105, at 631.

107. Scott J. Shackelford & Michael Mattioli, *Powerhouses: A Comparative Analysis of Blockchain-Enabled Smart Microgrids*, 46 J. CORP. L. 1003, 1007, 1015 (2021); *see also* Scott J. Shackelford, Michael Sulmeyer, Amanda N. Craig, Craig Deckard, Ben Buchanan & Brian Micic, *From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and What to Do About It*, 96 NEB. L. REV. 320 (2017).

108. *See, e.g.*, *Cyber-Attack Against Ukrainian Critical Infrastructure*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (July 20, 2021), https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [https://perma.cc/RN2D-TLHV].

109. Desai & Makridis, *supra* note 95.

Once again, consider the impact that the 2024 CrowdStrike incident had on the accessibility of critical infrastructure. Numerous sectors experienced outages around the world, including transportation, energy, and banking.[110] State-sponsored attackers have used software updates in the past to infiltrate systems in coordinated supply chain attacks, such as the one targeting SolarWinds and Microsoft Exchange.[111] The potential for widespread disruption utilizing weaponized updates should not be understated, nor should the risks associated with unanticipated errors, such as the CrowdStrike incident. A coordinated approach to enhance security across the software ecosystem is essential to begin to address the technical debt plaguing critical infrastructure systems, and to ensure that the situation does not worsen.

An alternative approach to the sector-specific status quo would consider the network structure across nodes, e.g., sub-sectors and firms. Desai and Makridis leverage data on industry-to-industry economic links to construct a measure of the value chain for cybersecurity.[112] Using data on vulnerabilities from Rapid7 among Fortune 500 companies, they find that, after accounting for the indirect effects of one sector on another, professional services rank the greatest in number of vulnerabilities. That is because every sector relies on professional services, and there are often choke points, i.e., certain nodes in an ecosystem that matter much more than others in determining the aggregate flow of economic activity.

E. Illustrative Example: AI-Enabled Content

The integration of generative AI in code development introduces both severe challenges and transformative opportunities. Generative AI has enabled software developers to produce content, including code, at unprecedented scales and speeds. Through natural language processing models, generative AI tools can generate entire scripts, functions, and even complex systems architecture, offering the capability to automate parts of the coding process that once required extensive human labor. For firms looking to scale their technology or rapidly prototype new solutions, this represents a major leap forward. However, the automation of code generation comes with an increased risk profile, where AI-generated code can introduce vulnerabilities, which may be exploited by malicious actors.

AI-generated content, due to its reliance on probabilistic models and datasets not always optimized for cybersecurity, can be more susceptible to offensive cyber maneuvers. A growing body of literature has found that generative AI's outputs—by design, often intended to generalize patterns and complete prompts—can inadvertently overlook nuanced security requirements. Offensive cyber capabilities, such as adversarial attacks, exploit these vulnerabilities, leveraging AI's generalized training to trick or circumvent system defenses. In fact, initial studies suggest that generative AI has become a tool that disproportionately benefits attackers over

---

110. *CrowdStrike Update Leads to Disruption Across Critical Infrastructure Environments*, INDUS. CYBER (July 19, 2024), https://industrialcyber.co/it-ot-collaboration/crowdstrike-update-leads-to-disruption-across-critical-infrastructure-environments/ [https://perma.cc/5525-Z8NN].

111. U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-104746, CYBERSECURITY: FEDERAL RESPONSE TO SOLARWINDS AND MICROSOFT EXCHANGE INCIDENTS (2022).

112. Desai & Makridis, *supra* note 95.

defenders, as malicious actors exploit the predictable or pattern-based outputs of generative models to penetrate systems, access sensitive data, or disable protective features.[113] This asymmetry in AI's defensive versus offensive utility represents a critical area of concern, prompting calls for specialized security layers in AI-generated code environments and regulatory guidance.

Another issue is the role of AI in software updates, particularly where AI-driven automation is employed to create or distribute patches without thorough human oversight. The CrowdStrike incident shows how the rapid deployment of updates, while aimed at improving functionality or security, can produce unintended consequences if inadequately tested.[114] The centralization of AI in generating and implementing updates amplifies the risks, as a single error in the code generation or deployment logic can cascade across interconnected systems, disrupting critical operations. This problem is magnified in AI-managed systems where updates may lack rigorous, context-specific testing, as was the case in the CrowdStrike deployment that caused widespread disruptions in critical infrastructure sectors. The increasing reliance on AI in update processes raises essential questions about accountability, as automated deployments may outpace human capacity for real-time quality assurance, particularly when patches or updates are pushed automatically without the option for manual review.

Regulation has been slowly trying to catch up to these contemporary possibilities. For example, a California law, Assembly Bill 331 ("AB 331"), sought to establish regulatory guardrails around AI in ways that would have set a precedent for AI oversight in the United States. AB 331, which nearly passed in 2023, would have mandated transparency and accountability standards for companies using "high-risk" AI systems, requiring them to assess and mitigate potential risks, including those tied to discrimination, security vulnerabilities, and privacy breaches largely following the EU approach discussed in Part III. In practice, these requirements would have made California one of the first U.S. states to require companies to undergo AI risk assessments and disclose how they handle sensitive data in AI systems. The proposed legislation classified AI systems as "high risk" if they significantly impact public welfare, such as through facial recognition, large-scale data processing, and systems with cybersecurity implications.

One of the most impactful provisions of AB 331 included a requirement that companies conduct regular assessments of their AI systems to identify and mitigate security risks and ensure AI-generated content did not introduce vulnerabilities, a pressing concern as AI begins to generate code and make operational decisions in real time. The bill also would have required a reporting mechanism to monitor and evaluate unintended outcomes, effectively creating a framework for AI oversight that

---

113. *See, e.g.*, Maha Charfeddine, Habib M. Kammoun, Bechir Hamdaoui, and Mohsen Guizani, *ChatGPT's Security Risks and Benefits: Offensive and Defensive Use-Cases, Mitigation Measures, and Future Implications*, 12 IEEE Access 30263, 30299 (2024); *cf.* CBS Mornings, *Cybersecurity Expert Says Advancements in AI Will Increase Cyber Threats in 2024*, YOUTUBE (Jan. 2, 2024), https://www.youtube.com/watch?v=CcqkmYVUL2g.

114. *See* Katie O'Flaherty, *CrowdStrike Reveals What Happened, Why—And What's Changed*, FORBES (Aug. 7, 2024), https://www.forbes.com/sites/kateoflahertyuk/2024/08/07/crowdstrike-reveals-what-happened-why-and-whats-changed/ [https://perma.cc/TBJ6-3UQ8].

echoed some of the EU's proposals under the AI Act, though AB 331 did not reach the same level of specificity in enforcement mechanisms. However, the bill faced pushback from tech companies and industry groups concerned about the regulatory burden it would place on innovation and the potential constraints on small businesses. Ultimately, AB 331 fell short in the state Senate, but it has remained an illustrative example of the type of regulatory framework that could pass to advance certain standards.[115]

III. COMPARATIVE CASE STUDIES

This Part builds from the legal theories and applications discussed in Part II and globalizes the discussion by considering how a range of leading cyber powers including the European Union, the United Kingdom, Singapore, India, and China are approaching this topic. Areas of convergence and divergence are then highlighted, with implications for policymakers discussed in Part IV.

A. European Union

The European Union has adopted a more comprehensive and expansive approach to holding software developers liable compared to the commonly discussed frameworks in the United States. Recognizing that many products—from toasters to cars—have become increasingly "smart," the European Union initiated an update to its products liability rules in 2022.[116] This revision, addressing a framework largely unchanged since 1985, broadens the definition of "product" to include not only hardware but also stand-alone software, such as firmware, applications, and computer programs, along with AI systems.[117] Certain exemptions apply to free and open-source software, a long-standing focus for advocates of stricter software liability.[118] Similarly, the definition of "defect" has been broadened to encompass cybersecurity vulnerabilities, including failures to implement patches.[119] The idea of what constitutes "reasonable" cybersecurity—such as a product failing to meet expected service levels—draws from other EU acts and directives, as discussed further below.

Recovered damages have also broadened to include the destruction or corruption of data, along with mental health impacts following a breach. Covered businesses can also include internet platforms with the intent being that there is always an "EU-

115. However, California did pass new laws on AI transparency, along with new protections against the unauthorized use of digital replicas, and AI labeling. *See* M. Oren Epstein, Stuart D. Levi, Glen G. Mastroberte, Priya R. Matadar & Shannon N. Morgan, *California Enacts Host of AI-Related Bills Designed to Protect Individuals*, SKADDEN (Sept. 25, 2024), https://www.skadden.com/insights/publications/2024/09/california-enacts-host-of-ai-related-bills [https://perma.cc/9VVY-L8JM].

116. *See* New Products Liability Directive, EUR. PARL. DOC. (COM 495) (2023).

117. *Id.* at 4–5.

118. *Id.* at 6.

119. *Id.*

based business that can be held liable."[120] Even resellers who substantially modify products and put them back into the stream of commerce may be held liable. It's now also easier for Europeans to prove their claims through the introduction of a more robust U.S.-style discovery process and class actions, along with easing the burden of proof on claimants and extending the covered period from ten to twenty-five years in some cases.[121]

Although the European Union has long been a global leader on data governance and products liability, the same has not necessarily been the case for cybersecurity—particularly pertaining to critical infrastructure protection. In 2016, the European Union worked to change that through the introduction of the Network Information Security (NIS) Directive, which was updated in 2022 as NIS2.[122]

Among other things, NIS2 expanded the scope of coverage to new "essential" and "important" sectors including cloud and digital marketplace providers, required EU member states to designate Computer Security Incident Response Teams (CSIRTs) and join Cooperation Groups, which are in essence international information sharing and analysis centers, or ISACs. Covered businesses must take appropriate steps to safeguard their networks, secure their supply chains, and notify national authorities in the event of a breach. In sum, NIS2 regulates software in a manner more familiar in the U.S. context, relying on information sharing and a risk management approach to standardize common activities like incident reporting.[123]

Further, the European Union's Cybersecurity Act, which took effect in June 2019, establishes a comprehensive framework for the certification of cybersecurity across information and communications technology products, services, and processes. The regulation aims to bolster trust in the digital market by ensuring that these entities adhere to standardized cybersecurity criteria. This certification scheme is voluntary, but it affects manufacturers and service providers by enabling them to demonstrate their compliance with high levels of cybersecurity, thereby enhancing market perception and consumer trust in their offerings. The Act fits within the broader EU strategy of leveraging regulatory measures over direct state control, epitomized by the role of European Union Agency for Cybersecurity (ENISA). ENISA has become a major entity in shaping and supporting the cybersecurity landscape across the European Union, despite facing challenges in establishing its authority and influence.[124]

From a products liability perspective, the Cybersecurity Act shifts the landscape by integrating cybersecurity into the core criteria for product safety and performance evaluations. By adhering to established certification standards, companies not only mitigate the risks of cyber threats but also reduce potential legal liabilities associated

---

120. Press Release, European Commission, Better Protection for Consumers Against Damages by Defective Products (Sept. 10, 2023).

121. *Id.*

122. Council Directive 2022/2555, 2022 O.J. (L 333/80).

123. *See Understanding the NIS2 Directive: Strengthening Cybersecurity in the European Union*, OPSWAT (Dec. 1, 2023), https://www.opswat.com/blog/understanding-the-nis2-directive-strengthening-cybersecurity-in-the-european-union [https://perma.cc/JB7C-J4RG].

124. Myriam Dunn Cavelty & Max Smeets, *Regulatory Cybersecurity Governance in the Making: The Formation of ENISA and Its Struggle for Epistemic Authority*, 30 J. EUR. PUB. POL'Y 1330 (2023).

with cybersecurity failures. The Act encourages transparency and accountability in cybersecurity practices, pushing companies to proactively manage and disclose cyber risks, which can influence their liability in cases of cyber breaches.

This approach aligns with the European Union's broader regulatory security state model, which emphasizes governance through regulation and expertise rather than through direct governmental intervention. This model is characterized by the deployment of indirect regulatory tools and reliance on the expertise and performance of various stakeholders to manage security issues, rather than solely depending on direct state power and authority. The voluntary standards have posed challenges, leading to uneven adoption and vulnerabilities in products not compliant with these standards and minimum security objectives for organizations. Nevertheless, some studies have commented that at least the Act has helped the European Union behave in a coordinated way.[125]

1. Adopting a "Secure by Design" Approach

In addition to the proposal to include software within the scope of products liability legislation, the European Union has introduced unified cybersecurity requirements for products sold within the common market, which includes pure software products. The Cyber Resilience Act (CRA),[126] a forthcoming EU regulation, combines detailed cybersecurity requirements, such as patch management and secure-by-design principles, with a comprehensive liability regime. The CRA can be considered as more comprehensive than California's "Internet of Things" (IoT) security law as the CRA's cybersecurity requirements go far beyond California's reasonable security features and password requirements, and the CRA applies to both IoT and software products.[127]

Fundamentally, the CRA requires that products be introduced to the market with all known vulnerabilities patched and that they have been developed under a secure by design basis. However, developers are also required to conduct and maintain a cybersecurity risk assessment, provide a software bill of materials listing out the third-party software components used in their products, and ensure security updates are available for a period of at least five years.[128] Developers and manufacturers of ordinary products can self-certify conformity with the legislation, while important and critical products will require a more in-depth assessment and an independent conformity assessment, respectively.

Noncompliance with the CRA follows the model used in the GDPR and can result in a fine of up to 15 million euros or 2.5% of total revenue (whichever is larger) for breaches of core requirements, while other breaches can result in a fine of up to 10

---

125. Donald David Stewart Ferguson, *European Cybersecurity Certification Schemes and Cybersecurity in the EU Internal Market*, INT'L. CYBERSECURITY. L. REV. 51 (2022).

126. 2024 O.J. (L 2847).

127. S. 327, Reg. Sess. (Cal. 2018).

128. 2024 O.J. (L 2847); *Council of the European Union Adopts the Cyber Resilience Act*, HUNTON (Oct. 17, 2024), https://www.hunton.com/privacy-and-information-security-law/council-of-the-european-union-adopts-the-cyber-resilience-act [https://perma.cc/QT3K-7XGA].

million euros or 2% of total revenue.[129] However, there is no mechanism under the Act for a complainant to enforce the CRA directly, and complainants must petition their local regulator if they believe the requirements have not been met.

2. Enhancing Transparency and Accountability Through Regulatory Frameworks

The EU's AI Act introduces a regulatory framework to protect users from harms caused by the failure of an AI system in the name of safety and transparency.[130] The Act classifies AI systems into three categories—prohibited, high-risk, and non-high-risk—and is reminiscent of the CRA in its comprehensive scope.[131] Prohibited applications, such as those involving subliminal techniques or social scoring, are banned within the European Union. High-risk applications, which include medical devices and credit scoring systems, must adhere to stringent requirements, including maintaining a risk management system, ensuring human oversight, and registering in the EU's database of high-risk AI systems. Non-high-risk applications face minimal to no regulatory obligations.

The Act also addresses general purpose AI models, like foundation and large language models, imposing obligations similar to those for high-risk systems. These include maintaining a copyright policy and publishing a summary of the training data. Enforcement is managed by domestic regulators and coordinated at the EU level by the newly established European Artificial Intelligence Board and the European Office for AI, where complaints can also be lodged against noncompliant AI providers.[132]

There are penalties for noncompliance. Violations involving prohibited AI can result in fines up to 30.3 million euros or 7% of total revenue.[133] High-risk AI breaches may lead to fines of up to 15.14 million euros or 3% of total revenue, and providing misleading information to regulators can attract fines up to 7.5 million euros or 1.5% of total revenue.[134] The applicable fine, higher or lower, depends on whether the entity is a large corporation or a small to medium-sized enterprise. One of the major limitations in the EU's AI liability regime, however, exists in its broad categorization of risk. In reality, there are many different dimensions of risk, let alone the definition of fairness in AI systems. In particular, the explainability and interpretability of AI systems are often used interchangeably, and that language will make it difficult to enforce and promote trustworthy AI practices.[135]

In the event that a user is harmed following their use of a high-risk AI system, they will be able to benefit from a proposed companion directive, which introduces

---

129. 2024 O.J. (L 2847) art. 64, 3.

130. EUR. PARL. DOC. (COM 0138) (2024).

131. *Cyber Resilience Act Product Categories*, CYBER CERT. LABS, https://www.cybercertlabs.com/case_studies/cra-categories/ [https://perma.cc/9QBP-LC8K].

132. *Id.*

133. 2024 O.J. (L 2847) art. 99, 4.

134. *Id.*

135. Mike H.M. Teodorescu & Christos Madrikis, *Fairness in Machine Learning: Regulation or Standards?*, BROOKINGS INST. (Feb. 15, 2024), https://www.brookings.edu/articles/fairness-in-machine-learning-regulation-or-standards/ [https://perma.cc/N8AT-9STC].

additional civil liability requirements for AI systems.[136] Under the proposed directive, the user will be able to seek a court order compelling the provider of the AI system to disclose relevant evidence relating to the suspected harm.[137] However, the claimant will be required to demonstrate to the relevant court that the provider has failed to comply with its obligations under the AI Act in order for their claim to succeed. Harm that occurs to the claimant despite the provider meeting its obligations under the AI Act is not recoverable under this legislation.[138]

This approach, as is the case with data privacy in the EU context, is far more comprehensive than the Biden administration's AI executive order and sets out accountability and transparency rules that are already shaping global AI governance.[139]

As with the AI Act, the GDPR is a comprehensive data protection law. It came into effect in the European Union on May 25, 2018, aiming to empower individuals with sovereignty over their personal data and simplify the regulatory environment for business. In particular, the GDPR requires that companies that process personal data be accountable for handling it securely and responsibly. This includes ensuring that data processing is lawful, fair, transparent, and limited to the purposes for which it was collected. Product and service providers must disclose their data processing practices and seek explicit consent from users in many cases, making them directly liable for noncompliance. The GDPR also gives individuals the option of demanding that a company delete their personal data or transfer it to another provider.

Although there are penalties for noncompliance for both primary data controllers and potential third parties, it has been very difficult to enforce and prove liability. For example, the European Union's own internal analysis has explained how international data cooperation has been challenging due to factors like "lack of practice, shortcomings in the legal framework, and problems in producing evidence."[140] Furthermore, since consumers often are searching for specific information and do not have other options, they simply consent to the relevant disclaimers on a site to enter and never think twice about the data that was shared and/or the possibility of filing a lawsuit against a company for potential damages from, say, a data breach.[141]

---

136. *Commission Proposal for a Directive of the EU Parliament and of the Council on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive)*, COM (2022) 496 final (Sept. 28, 2022).

137. *Id.*

138. *Id.*

139. *See* Mohamed Elbashir, *EU AI Act Sets the Stage for Global AI Governance: Implications for US Companies and Policymakers*, ATL. COUNCIL (Apr. 22, 2024), https://www.atlanticcouncil.org/blogs/geotech-cues/eu-ai-act-sets-the-stage-for-global-ai-governance-implications-for-us-companies-and-policymakers/ [https://perma.cc/TQG4-LJ49].

140. MILIEU CONSULTING SRL, STUDY ON THE ENFORCEMENT OF GDPR OBLIGATIONS AGAINST ENTITIES ESTABLISHED OUTSIDE THE EEA BUT FALLING UNDER ARTICLE 3(2) GDPR 47 (2023), https://www.edpb.europa.eu/system/files/2023-04/call_9_final_report_04112021_en_0.pdf [https://perma.cc/CLR7-PH4X].

141. *See* Matt Burgess, *What Is GDPR? The Summary Guide to GDPR Compliance in the UK*, WIRED (Mar. 24, 2020), https://www.wired.com/story/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018/ [https://perma.cc/4DMU-MMGY]; MILIEU CONSULTING

Furthermore, empirical studies generally point toward a negative effect of the GDPR on economic activity and innovation. Some studies have found that the GDPR led to a decline in new venture funding and new ventures, particularly in more data-intensive and business-to-consumer sectors.[142] Others found that companies exposed to the GDPR incurred an 8% reduction in profits and a 2% decrease in sales, concentrated particularly among small and medium-sized enterprises.[143] There is additional evidence that the GDPR led to a 15% decline in web traffic and a decrease in engagement rates on websites.[144]

Finally, the Digital Services Act (DSA) regulates online intermediaries and platforms such as "social networks, content-sharing platforms, app stores, . . . online travel and accommodation platforms[,] . . . [and] online marketplaces."[145] It took effect in a staggered process in 2022 and promised risk reduction, democratic oversight, and improvement of online rights. Articles 6(1), 9(1), and 22 of the DSA could be significant after cyberattacks, while Articles 17 through 21 could be crucial protections for users of online platforms whose accounts are suspended or terminated due to intrusions or misuse attributable to cyber threats. Article 9(1) obliges certain platforms to remove illegal material upon being served with notice of specific items by "judicial or administrative authorit[ies]."[146] Regarding online dangers other than intellectual property infringement and incitement to violence, Recital 12 of the DSA references "stalking" and "the unlawful non-consensual sharing of private images."[147]

SRL, *supra* note 140, at 47.

142. *See* Jian Jia, Ginger Zhe Jin, Liad Wagman, *The Short-Run Effects of the General Data Protection Regulation on Technology Venture Investment*, 40 MARKETING SCIENCE 593, 662–64 (2021) (reporting a decline of in such ventures and venture funding of about 11% to 31% and noting that a previous study found that new firms are most adversely affected by privacy regulation).

143. *See* Chinchih Chen, Carl Benedikt Frey & Giorgio Presidente, *Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally* (Oxford Martin Working Paper Series on Tech. & Econ. Change, Working Paper No. 1, 2022), https://oms-www.files.svdcdn.com/production/downloads/Privacy-Regulation-and-Firm-Performance-Giorgio-WP-Upload-2022-1.pdf [https://perma.cc/YWZ6-LZAD].

144. *See* Raffaele Congiu, Lorien Sabatino & Geza Sapi, *The Impact of Privacy Regulation on Web Traffic: Evidence From the GDPR*, 61 INFO. ECON. & POL'Y 1, 2 (2022); Jia et al., *supra* note 142, at 663–64.

145. *The Digital Services Act*, EUR. COMM'N (Oct. 27, 2022), https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en [https://perma.cc/A6PA-996D].

146. Digital Services Act, art. 9(1), 2022 O.J. (L 277).

147. EUROJUST, DIGITAL SERVICES ACT: ENSURING A SAFE AND ACCOUNTABLE ONLINE ENVIRONMENT (2022), https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-digital-services-act-factsheet-11-2022.pdf [https://perma.cc/8SN5-WZNK]; *How the Digital Services Act Enhances Transparency Online*, EUR. COMM'N, https://digital-strategy.ec.europa.eu/en/policies/dsa-brings-transparency (Jan. 8, 2025) [https://perma.cc/87LN-UDMP].

In the United States, the law on loss of access to online accounts remains a patchwork, even in cases involving data breaches covered by federal statutes.[148] While some courts allow breach of express or implied contract as a theory of recovery, others may not, and arbitration clauses are a formidable challenge in some cases. Articles 20(4) and 21 of the DSA strengthen the right to use online platforms and not to suffer arbitrary deprivation of access.[149]

Settlements of class actions like those involving iPhone battery life and Google Chrome incognito mode do suggest that defective software and misleading marketing of technology claims have traction in U.S. courts without further reforms.[150] Products liability and data security litigation remains viable due to the similarity of many U.S. states' laws and the intention of the federal class-action procedure to make asserting small-dollar claims economical.[151]

B. UK

Looking beyond the EU, and to the United Kingdom (UK), harm or damage to a person or their property arising from a product, caused by a manufacturing design fault or defect,[152] are covered mainly by the Products Liability Directive.[153] This piece of legislation has, at the time of writing, been in place for thirty-nine years, and it was introduced when the UK was part of the European Economic Community, the forerunner to the European Union. As the UK has left the European Union, PLD2 will not take effect, and the UK remains, at the time of writing, with the Products Liability Directive.

The Products Liability Directive (PLD) creates a strict/no-fault liability regime, which allows a consumer to seek compensation for material harm or damage caused

---

148. *See In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304 (D. Minn. 2014); *see also* Caroline Ribet, *Don't Just Do Something, Stand There: What Criminal Law Teaches Us About Article III Standing in Data Breach Cases*, 172 PENN. L. REV. 257, 275–285 (2023).

149. Digital Services Act, arts. 20(4), 21, 2022 O.J. (L 277).

150. *See* Press Release, Attorney General, Department of Justice, State of California, Attorney General Becerra Announces $113 Million Multistate Settlement Against Apple for Misrepresenting iPhone Batteries and Performance Throttling (Nov. 18, 2020) https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-113-million-multistate-settlement-against [https://perma.cc/WUD8-XH5E]; Lauren Feiner, *Google Agrees to Destroy Browsing Data Collected in Incognito Mode*, THE VERGE (Apr. 1, 2024), https://www.theverge.com/2024/4/1/24117929/google-incognito-browsing-data-delete-class-action-settlement [https://perma.cc/L2NT-ZKCZ].

151. *See, e.g.*, Phillips Petroleum Co. v. Shutts, 472 U.S. 797 (1985).

152. Although the term "design defect" echoes that which has been used in the American courts, and has been ruled out as an approach in the UK's approach to products liability, *see, e.g.*, Commentary, *Consumer Protection Act 1987: Liability For Defective Products,* 10 MED. L. REV. 82, 86–87 (2002), the use of the phrase here is solely explanatory and not indicative of any legal mechanism.

153. Council Directive 85/374/EEC on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products, 1985 O.J. (L 210/29). In the UK, the 1985 Directive has been transposed into domestic law via the Consumer Protection Act 1987, c. 43, § 1.

by the defective products,[154] where the product has not provided the safety which a person is entitled to expect,[155] subject to the conditions of the directive, such as the claim being within three years of injury and less than ten years after the product has been launched.[156] Injury or harm which occurs after the ten years is out of the scope of the strict liability regime.[157]

It has been noted that products liability is an area of law in which there are (relatively) few cases taken. One explanation for this is:

> Due to the high costs involved in filing products liability cases, including court fees and attorney's fees, and the difficulty in acquiring evidence from the manufacturer or producer to prove the defect, the imposition of strict liability upon proof of the defect, damage and the causal relationship between the damage and the defect, irregardless of the care the manufacturer or producer exercised, strikes an appropriate balance of interest between the consumer and the producer, especially in developing countries.[158]

Pure, intangible software products are not explicitly covered by the PLD. However, the following analysis outlines the requirements which claimants must meet in order to achieve a finding of a defective product. Although limited in number, there have been products liability cases in the United Kingdom and the European Union which are relevant for discussing the issues related to establishing liability arising from a software defect. The *Stoke-On-Trent* case outlines clearly how once a claimant can demonstrate that the device is defective, then the product manufacturer will be liable for the damage or harm which is caused. Judge Davies notes how:

> [O]nce the claimant proves that the defendant has supplied electrical equipment which is unsafe and that the fire started as a result of that electrical equipment being unsafe then liability follows. There is a defence of due diligence available to a defendant in criminal proceedings (s.39(1) 1987 Act) but that does not apply to civil claims.[159]

---

154. In the UK, the threshold for damage to bring a claim is £275. Consumer Protection Act c. 43, § 5(4). In Ireland, the threshold is £350 (IEP) (~€406). Liability For Defective Products Act, 1991 (Act No. 28/1991). In both countries, there has been no provision to allow for non-material injuries, such as stress, to be used as the basis of a claim. *See id.*; Consumer Protection Act c. 43, § 5(4) (UK).

155. Council Directive 85/374/EEC, 1985 O.J. (L 210/29).

156. *Id.* at art. 10 (1, 2).

157. Wilson v. Beko PLC [2019] EWHC 3362 (QB) 10.

158. Katrina P. Borra, *Products Liability in the 21st Century*, JURID. REV. 199, 212 (2013).

159. Stoke-On-Trent College v. Pelican Rouge Coffee Solutions Group Ltd. [2017] EWHC 2829 (TCC) 139. It must be noted that this quotation is referring to regulations introduced in 1994, which were drafted to outline specific safety requirements for electrical equipment. These regulations were introduced via § 1 of the Consumer Protection Act 1987, which, as already mentioned in this Section, is a transcription of the 1985 Products Liability Directive.

This provides robust protection for the owner or operator of a product which contains software, following harm arising from a defect in the software which causes them harm or damage.[160]

A defect is defined in the PLD[161] as:

> [a circumstance] when [a product] does not provide the safety which a person is entitled to expect, taking all circumstances into account, including:
> (a) the presentation of the product;
> (b) the use to which it could reasonably be expected that the product would be put;
> (c) the time when the product was put into circulation.[162]

Accordingly, once a claimant has been able to successfully demonstrate that a defect is present, they will be in a strong position to ground a claim. The case of *Abouzaid* examines the nature of a defect in detail.[163] Here, a claim was brought against the defendant, Mothercare, on the basis that their product, a buggy, was defective as it required the owner to secure an elasticated strap in a manner where it was likely to slip from the owner's fingers which would result in the metal buckle being propelled with considerable speed and force back into the owner's person. Such an action happened to the defendant, whose eye was severely damaged as a result.[164] It was put forward by the defendant that since this action had happened nine years after the release of the product, and there had been no reports of such an action happening prior to this, the product was not defective, and this was just an isolated accident.

However, this defense was not held as viable by either the trial judge or the court of appeal.[165] It was determined that since the action which caused the harm had happened, the product was defective, and that the failure of the defendant to countenance such an action was itself not a defense (this point was made in conjunction with the fact that it would have been effectively trivial for the defendant to amend the design so as to remove the defect). As such, a claimant does not need to demonstrate that the defect has affected other people to mount a successful claim, merely that the alleged defect does in fact constitute a defect in the product.[166]

There are, however, defenses which are available to the producers of products under the PLD. The first of these is that the defect was not present in the device at the "relevant time."[167] This is examined in the case of *Richardson*, where the claim

---

160. *Id.*

161. The definition is taken from the Council Directive, 85/374/EEC, art. 6(1) 1985 O.J. (L 210/29), as opposed to the Consumer Rights Act 1987 following the decision of Comm'n v. United Kingdom, Case C-300/95, 1998 E.C.R. I (holding that any national legislation was to be construed as being in conformity with the Directive).

162. Council Directive 85/374/EEC, art. 6(1) 1985 O.J. (L 210/29).

163. Abouzaid v. Mothercare (UK) Ltd., [2000] EWCA (Civ.) J1221-10 (appeal taken from Eng.).

164. *Id.* ¶¶ 3–5.

165. *Id.* ¶¶ 32–33.

166. *Id.*

167. Consumer Protection Act 1987, c. 43, § 4(1)(d).

that a condom was defective due to it having split during intercourse was rejected, as it was not possible (nor probable, given the expert testimony) that the split was a result of a defect which took place during the manufacturing process, but instead was a result of some action that happened post sale, and so there was no defect in the product at the time of sale.[168]

As such, it is clear how the mere fact of harm does not automatically ensure that the device is defective. The claimant must be able to demonstrate their harm was a result of a defect in the product at the time of manufacturing. Accordingly, it is clear how the finding in *Richardson* can be considered as a high hurdle for claimants to clear with regards to alleged defective software, where the harm has arisen following a cybersecurity failure. This is because cyberattackers will normally alter the coding and data on the product during their attack. The claimant will need to demonstrate that the cyberattacker leveraged a defect which was present in the product at the time when it was released to the market, and which allowed the cyberattackers to cause the harm.[169] This point is discussed in detail further on in this chapter.

The second defense relates to the state of technical knowledge at the time of sale and provides a defense if "the state of scientific and technical knowledge at the relevant time was not such that a producer of products of the same description as the product in question might be expected to have discovered the defect if it had existed in his products while they were under his control."[170] This defense is known as the "development risks" defense.

The case of *A and Others v. National Blood Authority* examines this defense in detail.[171] From the case, it is clear that if a defect has been already "discovered," then such a defense is not available to a defendant.[172] However, if the defect was not known at the time of the production launch, due to it not being reasonable for the manufacturer to know about the defect given the current state of scientific and technical knowledge, the manufacturer will not be liable for harm caused by the defect. It has been noted how the challenge in bringing the development risks defense is whether an unknown defect was "reasonably discoverable" by the manufacturer at the time of the product's release.[173] This challenge was examined in *A,* and draws heavily from the non-binding but influential Advocate General's opinion in the case of the *Commission v. United Kingdom*, which equated the concept of "knowledge" with scientific and technical journals.[174] However, Judge Burton also included unpublished research documents in this definition.[175] Furthermore, general knowledge and an awareness of current events has also been included in the

---

168. *Richardson v. LRC Products Ltd*, PERS. INJS. Q. REV. 164 (2000).

169. *See* Council Directive 85/374/EEC, art. 8, 1985 O.J. (L 210/29) (confirming that the liability of the manufacturer is not reduced when the harm or damage is a result of both a defect and the act or omission of a third party).

170. Consumer Protection Act 1987, c. 43, § 4(1)(e).

171. A v. Nat'l Blood Auth. [2001] EWHC (QB) 446 [¶ 48] (Hepatitis C Litigation).

172. *Id.* at 74, ¶¶ 19–21.

173. *See* Charles Pugh & Marcus Pilgerstorfer, *The Development Risk Defence—Knowledge Discoverability and Creative Leaps*, J. PERS. INJ. L. 258, 267 (2004).

174. *See* Case C-300/95, Comm'n v. United Kingdom, 1998 E.C.R. I-2649.

175. *See* A v. Nat'l Blood Auth. [2001] EWHC (QB) 446, at ¶ 49.

definition of knowledge, even when it pre-dates a formal publication.[176] It is not, however, possible for a claimant to invalidate the development risks defense by demonstrating merely that there was pre-existing evidence of the defect somewhere within the scientific or general literature, instead, it must be demonstrated that the producer of the good can objectively be expected to be aware of that specific knowledge.[177]

From the perspective of a software developer, and the cybersecurity risks outlined earlier in this Article, the finding of *A* would suggest that if a producer was unaware of a defect within their software, and this defect was caused by a vulnerability which had been reported and discussed by other users of that technology, the development risks defense would not likely be available to the producer.

The development risks defense may be somewhat academic in the context of software, as the software used in many products is normally either comprised of off-the-shelf components and therefore well known,[178] and thus defects are either known or discoverable. The same is true for software which relies upon open-source components.[179] There are, of course, exceptions where a producer has developed an entirely novel hardware or software component, but the defendant would need to show the equivalent of a "zero day" (a completely novel) defect in order to claim this defense.

From this, we see how there are robust (and generally accepted as adequate)[180] protections for consumers who are sold products which are defective and whose defect has resulted in harm or damage to the consumer. However, has it been established that a defect which arises from the software component of a product falls within scope of the PLD?

A leading case which potentially answers this question is *Krone.*[181] In *Krone*, the question as to whether a person who had purchased a newspaper which contained an

---

176. *See, e.g.*, Pugh & Pilgerstorfer, *supra* note 173, at 261 (discussing "magnetic catches").

177. Case C-300/95, Comm'n v. United Kingdom, 1998 E.C.R. I-2649.

178. Ahmad Majid Qazi, Syed Hasan Mahmood, Abid Haleen, Shashi Bahl, Mohd Javaid & Kanu Gopal, *The Impact of Smart Materials, Digital Twins (DTs) and Internet of Things (IoT) in an Industry 4.0 Integrated Automation Industry*, 62 MATERIALS TODAY: PROCS. 18 (2022); Chi-Yu Chen, Chun-Liang Lin & Yang-Yi Chen, *Realization of Ideal Architecture of IoTs*, 14 ARRAY 1 (2022); *see, e.g.*, Wafa'a Kassab & Khalid A. Darabkh, *A–Z Survey of Internet of Things: Architectures, Protocols, Applications, Recent Advances, Future Directions and Recommendations*, 163 J. NETWORK AND COMPUT. APPLICATIONS 102663 (2020).

179. *See, e.g.*, PETER WEIDENBACH & JOHANNES VOM DORP, HOME ROUTER SECURITY REPORT 2020, FRAUNHOFER (2020), https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf [https://perma.cc/YCL8-8TLA]; Bruce Schneier, *Router Security*, SCHNEIER ON SEC. (Feb. 19, 2021), https://www.schneier.com/blog/archives/2021/02/router-security.html [https://perma.cc/2MJD-K8TE].

180. *See, e.g.*, Etienne Farnoux, *Going Beyond the Localisation of Damage in the Field of Product Liability*, INT'L BUS. L. J. 641 (2022); SWEET & MAXWELL, *Inaccurate Health Advice in Newspaper Does Not Give Rise to Liability Under Defective Products Directive*, 405 EU FOCUS 9 (2021).

181. Case C 65/20, VI v. KRONE-Verlag Gesellschaft mbH & Co. KG, ECLI

article which proposed incorrect health advice could seek redress from the newspaper manufacturer on the basis that the incorrect advice in the article rendered the newspaper "defective" was examined by the Court of Justice of the European Union (CJEU). While the CJEU reaffirmed that services do not fall under the scope of the Directive,[182] it was held that were a service to be presented and positioned to a consumer as an integral part of the product, then it could fall within scope of the Directive,[183] a position which has oft been argued, both before and after the *Krone* decision.[184] Accordingly, it is reasonably clear that under the PLD, if software which is fundamental to the operation of a product (as opposed to an additional service or independent application which is not a core component part of the product) is defective, the producer will be liable for any harm caused by the defect, subject to the defenses already discussed in this chapter.

Could a producer be held liable for the harm caused by a third party who exploited a technical defect in the software to use the device to cause harm? While this specific question has not yet come before a court, it seems clear that the answer must be "no." The reason for this would appear to be three-fold; firstly, Article 3 of the Directive defines a producer as being either the party who produced the product or (broadly speaking) a party who was involved in the sale of the product,[185] and so the producer, in general, is not responsible for actions of the third party which take place after the product has been released into the market.

Secondly, for a cyberattacker to take control of the product, it is very probable that they must alter the device's software in some way, such as by installing their own control software, de-activating modules in the operating system, or creating new user or administrative accounts. These changes, which would "allow" the product to become defective, are introduced after the product has been entered into the market, which is a defense against liability as the product was not defective when it was put into circulation.[186] This reflects the judgement in *Richardson*.[187] Accordingly, it is probable that the actions of the cyberattacker will not hold the producer liable to the owner or user of the product, let alone an unrelated third-party.

It is, however, interesting to note that such a defense may not hold where the cyber-attacker has exploited an existing defect in the product to carry out their harm. This would include a scenario where an attacker was able to compromise the software which was used in the manufacturing of the product, and thus it would be sold with malware embedded into the device, such as when USB keys issued by IBM were put into circulation when they contained malware, and as such were defective

---

:EU:C:2021:471 (June 10, 2021).

182. *Id.* ¶ 29.

183. *Id.* ¶¶ 32–36.

184. *See, e.g.*, Duncan Fairgrieve, *Reforming the European Product Liability Directive: Plus ça Change, Plus c'est La Même Chose?*, J. PERS. INJ. L. 33 (2019); K Alheit, *The Applicability of the EU Product Liability Directive to Software*, 34 COMPAR. & INT'L L.J. S. AFR. 188 (2001); John N. Adams, "*The Snark Was a Boojum You See": Beta Computers (Europe) Ltd v Adobe Systems (Europe) Ltd; St Albans City and District Council v International Computer Ltd*, 1 EDINBURGH L. REV. 386 (1997).

185. *See* Council Directive 85/374/EEC, art. 3, 1985 O.J. (L 210/29).

186. *Id.* at art. 7(b).

187. Richardson v. London Rubber Co. Prods. Ltd., (2000) 2 WLUK 78.

ab initio.[188] However, given how PLD defines a "defect" to be "the presentation of the product," "the use to which it could reasonably be expected that the product would be put," and "the time when the product was put into circulation,"[189] it is clear that the PLD is based around an individual choosing to purchase a product based on their perception of the product. Given how a remote third-party has neither purchased nor used the product, it is unlikely that they would be able to ground a claim; this ability would be reserved for users and owners of products.

There have also been examples of products which have been sold into the market and contained no mechanisms to prevent third parties from accessing and controlling the device.[190] Although never examined in the courts, this would likely be considered as a defect, since it is hard to argue that such a state represents the safety "which a person is entitled to expect."[191] However, one of the likely reasons why these millions of devices did not result in a claim under the PLD is that the defect did not harm the users or operators of the products in question, as the harm was suffered by third-parties. It is likely that most owners or users of the affected products were unaware of the defect, and as such, the PLD is not a viable mechanism to use to launch a claim as no harm occurred.

There is also the question as to whether a vulnerability in the software of a product, which allowed a cyber-attacker to gain access to and control the device, would constitute a defect under the PLD. If the product was manufactured and the vulnerability was known and reported on by other users of that hardware or software, such as to a vulnerability database, then it is hard to see how the development risks defense would hold. There remains the question as to whether a court would view the vulnerability as a defect, although there is a very large body of work which outlines how vulnerabilities in products are exploited by cyber-attackers in a very short space of time,[192] and how security updates are seen as a core constituent of cybersecurity.[193] However, as mentioned already, the claimant will also need to

---

188. *See, e.g.*, Danny Palmer, *IBM Warns of Malware on USB Drives Shipped to Customers*, ZDNET (May 2, 2017), https://zdnet.com/article/ibm-warns-of-malware-on-usb-drives-shipped-to-customers [https://perma.cc/FJB9-J3RS].

189. Council Directive 85/374/EEC, art. 6(1), 1985 O.J. (L 210/29) (describing the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products).

190. See, for example, Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou & Jeffrey Voas, *DDoS in the IoT: Mirai and Other Botnets*, 50 COMPUTER 80 (2017), for a discussion about how millions of products were sold with hard-coded administration passwords such as "Admin" and "Password," and which the user could not change. These were exploited by cyberattackers.

191. Council Directive 85/374/EEC on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products, 1985 O.J. (L 210/29).

192. *See, e.g.*, Danny Palmer, *IoT Devices Can Be Hacked in Minutes, Warn Researchers*, ZDNET (Oct. 16, 2016, 6:00 AM), https://www.zdnet.com/article/iot-devices-can-be-hacked-in-minuteswarn-researchers/ [https://perma.cc/7ZPC-Z26E].

193. *See, e.g.*, MICHAEL FAGAN, JEFFREY MARRON, KEVIN G. BRADY, JR., KATERINA N. MEGAS, REBECCA HEROLD, DAVID LEMIRE & BRAD HOEHN, IOT DEVICE CYBERSECURITY GUIDANCE FOR THE FEDERAL GOVERNMENT: ESTABLISHING IOT DEVICE CYBERSECURITY REQUIREMENTS (2021), https://doi.org/10.6028/NIST.SP.800-213 [https://perma.cc/JP9H-

demonstrate that the cyberattacker has caused them damage or harm, in order to mount such a claim. At the time of writing, it must be noted how there are no known successful claims brought against producers under the PLD.

Finally, we examine a related question. If a consumer is provided with a product, as part of the provision of a service, can the consumer seek redress directly from the manufacturer of the product in the event of the device having a defect? From *Dutrueux*, we know that if a party provides a service, and in the course of the provision of that service they use a faulty product, the recipient of the service is not able to use the PLD to seek compensation from the service provider or the product's producer.[194]

As such, it seems clear that consumers have some, albeit limited, recourse against defective products where the defect was caused by software. If the product is a software product, and the claimant can demonstrate the harm which the defect caused, and the nature of the defect itself, they could succeed with a claim under the PLD in the UK, although their position would be materially weaker than a similar claimant in the EU who brought a claim under the forthcoming PLD2, as this explicitly allows claims against pure software products, as well as allowing Member States to disapply the development risks defense.[195]

C. Singapore

Alongside the UK, Singapore has proven itself an effective global leader in AI governance, and has implemented numerous laws to address cybersecurity issues.[196]

SJGP]; NAT'L CYBER SEC. CTR., *Security in the Internet of Things (IoT)*, (Mar. 17, 2025) (Switz.), https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-iot.html [https://perma.cc/M8RY-ZNA2]; ENISA, *Baseline Security Recommendations for IoT: In the Context of Critical Information Infrastructures*, (Nov. 20, 2017), https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot [https://perma.cc/3FZX-3223]; MICHAEL FAGAN, KATERINA N. MEGAS, KAREN SCARFONE & MATTHEW SMITH, FOUNDATIONAL CYBERSECURITY ACTIVITIES FOR IOT DEVICE MANUFACTURERS, NIST INTERNAL REP. 8259 (2020), https://doi.org/10.6028/NIST.IR.8259 [https://perma.cc/E4X9-SQ7Z]; FTC, CAREFUL CONNECTIONS: KEEPING THE INTERNET OF THINGS SECURE, (Sept. 2020), https://www.ftc.gov/system/files/documents/plain-language/913a_careful_connections.pdf [https://perma.cc/3RGG-S4F8]; CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, INTERNET OF THINGS SECURITY ACQUISITION GUIDANCE, https://www.cisa.gov/sites/default/files/publications/20_0204_cisa_sed_internet_of_things_acquisition_guidance_final_508_1.pdf [https://perma.cc/AK89-AMW9]; INTERNET SOC'Y, *IoT Security for Policymakers*, (2018), https://www.internetsociety.org/resources/2018/iot-security-for-policymakers/ [https://perma.cc/XPK5-3N2G]; NAT'L CYBER SEC. CTR., *Device Security Guidance*, (2022), https://www.ncsc.gov.uk/collection/device-security-guidance/security-principles/provide-updates-securely [https://perma.cc/D2YV-9SF3].

194. Case C-495/10, Centre hospitalier universitaire de Besançon v. Dutrueux & Caisse primaire d'assurance maladie du Jura, ECLI:EU:C:2011:869, ¶ 39 (Dec. 21, 2011).

195. Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC (Text with EEA relevance), 2024 O.J. (L).

196. Scott J. Shackelford & Rachel Dockery, *Governing AI*, 30 CORNELL J.L. & PUB. POL'Y 279, 324 (2020).

In 2013, it established the Personal Data Protection Commission (PDPC)[197] to regulate enforcement of the Personal Data Protection Act of 2012 (PDPA), which established protective policies that businesses must abide by when collecting personal data.[198] In 2015, Singapore formed the Cyber Security Agency (CSA) to guard both public and private sector cyberspace.[199] Two years later, Singapore created the Defense Cyber Organization (DCO) to protect national information infrastructure against cyber threats.[200]

In 2018, Singapore passed the Cybersecurity Act to establish a legal framework for overseeing and maintaining national cybersecurity in Singapore. Four key objectives of the Cybersecurity Act included strengthening the protection of Critical Information Infrastructure (CII) against cyberattacks, authorizing the CSA to prevent and respond to cybersecurity threats and incidents, establishing a framework for sharing cybersecurity information, and creating a light-touch licensing framework for cybersecurity service providers.[201]

Also in 2018, the Monetary Authority of Singapore established the *Fairness, Ethics, and Accountability and Transparency Principles* (FEAT) to (a) provide the finance sector with baseline principles when making AI and data analytics decisions, (b) assist firms in "contextualising and operationalising" AI and data analytics governance, and (c) promote public trust in AI and data analytics.[202] Since its inception, FEAT has been updated twice (in 2019, and again in 2020) to better reflect two main goals: ensure that financial institutions' AI decision-making is articulated, transparent, and fair, and that AI solutions be human-centric.[203]

In 2019, Singapore released the first edition of the Model AI Governance Framework ("Model Framework") to provide private sector businesses with ethical

---

197. *See About Us*, PERS. DATA PROT. COMM'N SING., https://www.pdpc.gov.sg/who-we-are/about-us [https://perma.cc/J3YB-2WJU].

198. *See PDPA: The Singapore Data Protection Act of Singapore Explained*, PERFORCE (Jan. 1, 2021), https://www.perforce.com/blog/pdx/personal-data-protection-act-singapore-pdpa [https://perma.cc/JKN7-4MYH].

199. *Who We Are*, CSA SING., https://www.csa.gov.sg/about-csa/who-we-are/ [https://perma.cc/B4AC-WDGX].

200. Shackelford & Dockery, *supra* note 196, at 324–25; *see also Cyber Defense*, MINDEF SING., https://www.mindef.gov.sg/defence-matters/defence-topic/cyber-defence [https://perma.cc/T92U-MPS3]. The DCO is comprised of six subsectors; the Singapore Armed Forces (AF), Ministry of Defense (MINDEF), Defense Science and Technology Agency (DSTA), Defense Science Organization (DSO), Defense Industry, and Corporate IT and Internet-Facing Organizations. *Id.*

201. Cybersecurity Act 2018, No. 9 of 2018 (Sing.).

202. Ross P. Buckley, Dirk A. Zetzsche, Douglas W. Arner & Brian W. Tang, *Regulating Artificial Intelligence in Finance: Putting the Human in the Loop*, 43 SYDNEY L. REV. 43, 61 (2021); *see also Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector*, MONETARY AUTH. OF SING., at 3 (2018) [hereinafter *FEAT Principles*], https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf [https://perma.cc/3RNY-RZUT].

203. Buckley et al., *supra* note 202, at 61.

and governance standards when deploying AI solutions.[204] This early Model Framework converted "high level AI ethics principles into implementable measures for organisations to deploy AI responsibly."[205] An updated second edition was released in 2020,[206] which incorporated industry feedback.[207] Both editions focused on issues relevant to traditional (non-generative) AI,[208] like bias, misuse, and lack of explainability.[209]

In 2022, Singapore issued the Cybersecurity Code of Practice for Critical Information Infrastructure to define minimum controls that organizations must have in place to address cybersecurity risks, and provide a cybersecurity risk management framework that allows companies to identify, analyze, evaluate, and address such risks.[210] In 2024, an updated Generative AI Model Framework was released through the collaborative effort of the AI Verify Foundation (AIVF) and Infocomm Media Development Authority (IMDA).[211] This latest edition focuses on Generative AI which presents additional risks beyond those most relevant to traditional AI, including hallucination, copyright infringement, and value alignment.[212] This Generative AI Framework offers nine dimensions that policymakers, industry leaders, researchers, and the general public should consider in order to foster a more reliable Generative AI ecosystem: (1) Accountability,[213] (2) Data,[214] (3) Trusted

---

204. *See Singapore's Approach to AI Governance*, PDPC SING. (Nov. 3, 2023), https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework [https://perma.cc/9TT9-L68H].

205. *Responsible AI Boosts Consumer Trust and Business Growth in Singapore*, INFOCOMM MEDIA DEV. AUTH. (May 2, 2024) [hereinafter *Responsible AI*], https://www.imda.gov.sg/resources/blog/blog-articles/2024/04/responsible-ai-boosts-consumer-trust-and-business-growth-in-singapore [https://perma.cc/QZ23-8KDQ].

206. *See* MODEL ARTIFICIAL INTELLIGENCE GOVERNANCE FRAMEWORK SECOND EDITION, PDPC SING. (2020), https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf/ [https://perma.cc/L233-2PBD].

207. *Responsible AI*, *supra* note 205.

208. Charmian Aw, *Singapore Publishes Generative AI Model Governance Framework*, NAT'L. L. REV. (May 31, 2024), https://natlawreview.com/article/singapore-publishes-generative-ai-model-governance-framework [https://perma.cc/DK6K-9S9C].

209. *See* AI VERIFY FOUND., MODEL AI GOVERNANCE FRAMEWORK FOR GENERATIVE AI, 3 (2024) [hereinafter MODEL FRAMEWORK FOR GENERATIVE AI], https://aiverifyfoundation.sg/wp-content/uploads/2024/05/Model-AI-Governance-Framework-for-Generative-AI-May-2024-1-1.pdf [https://perma.cc/F6CS-NR8H].

210. *See* CYBER SEC. AGENCY SING., CYBERSECURITY ACT OF 2018: CYBERSECURITY CODE OF PRACTICE FOR CRITICAL INFORMATION INFRASTRUCTURE (2d ed., 1st rev. 2022), https://isomer-user-content.by.gov.sg/36/2df750a7-a3bc-4d77-a492-d64f0ff4db5a/CCoP---Second-Edition_Revision-One.pdf [https://perma.cc/ZL4Y-8K24].

211. *See generally* MODEL FRAMEWORK FOR GENERATIVE AI, *supra* note 209. Note that this latest edition was proposed by the AI Verify Foundation and Infocomm Media Development Authority (IMDA), building upon the earlier Model Framework.

212. *Id.* at 3.

213. *Id.* at 3 (incentivizing accountability throughout the AI supply chain, from developer to end-user).

214. *Id.* at 4 (ensuring data quality to mitigate the garbage in, garbage out phenomena).

Development and Deployment,[215] (4) Incident Reporting,[216] (5) Testing and Assurance,[217] (6) Security,[218] (7) Content Provenance,[219] (8) Safety and Alignment Research and Development,[220] and (9) AI for Public Good.[221] Like the 2019 and 2020 Model Frameworks, stakeholders are not required to follow the updated Model Generative AI Framework; However, this latest Framework encourages stakeholders to consider the creation, deployment, and accountability of Generative AI more holistically within the broader international realm.[222]

At present, Singapore has no specific legislation that governs products liability; instead, issues of products liability are generally dealt within under the purview of either common law manufacturer negligence or contract law.[223] Under the standard of negligence in Singaporean tort law, a duty of care is owed by suppliers to buyers. Any breach of that duty that results in a foreseeable physical injury or property damage could result in a successful suit by the injured buyer.[224] Alternatively, complainants relying on contract law to establish products liability must show the existence of a contract between buyer and seller, that an express or implied term of such contract has been breached, and that such breach caused damage to the complainant.[225] Breach of contract liability does not require a showing of fault; instead, strict liability is the appropriate standard.[226]

While no bill or legislation specifically depicts the impact of products liability on software or cybersecurity, Singapore updated the Cybersecurity Act with the 2024 passage of the Cybersecurity (Amendment) Bill ("CS Bill") to address liability.[227] This new legislation accounts for evolving business and technological models that include virtual systems and overseas critical information infrastructure (CII)

---

215. *Id.* (promoting the adoption of best practices in the development and deployment of AI).

216. *Id.* ("Establishing structures and processes to enable incident monitoring and reporting . . . .").

217. *Id.* (encouraging third parties to utilize third party testing and assurance to promote trust among end users).

218. *Id.* (recommending that existing frameworks for AI security be updated to address generative AI risks).

219. *Id.* (promoting transparency about "where and how content is generated").

220. *Id.* (encouraging global cooperation to invest in safety and alignment research and development to better align AI use "with human intention and values").

221. *Id.* (endorsing AI access, improvement, and development in sustainable ways that promote the public good).

222. *Id.* at 3; *see also* Aw, *supra* note 208.

223. Lim Chong Kin & Benjamin Gaw, *Product Liability and Safety in Singapore: Overview*, THOMAS REUTERS PRAC. L. (Mar. 1, 2023), https://uk.practicallaw.thomsonreuters.com/w-013-0001 [https://perma.cc/9F4A-FNBQ].

224. *Id.*

225. *Id.*

226. *Id.*

227. Cybersecurity (Amendment) Act 2024, No. 19 of 2024 (Sing.), https://sso.agc.gov.sg/Acts-Supp/19-2024/Published/20240704?DocDate=20240704 [https://perma.cc/CA5N-7M6Y].

owners,[228] expands the scope of reportable cybersecurity incidents,[229] the parties subject to the CS Bill,[230] and enhances administrative powers.[231] The CS Bill permits parties to bring civil actions against CII owners that fail to comply with the updated requirements of the Bill.[232]

Of interest, the 1996 case, *St Albans City and District Council v. International Computers Ltd.*,[233] laid the foundation that computer software be treated as a product.[234] However, the court limited such intent to only computer software issued in physical form (like a computer disc), thereby excluding software that is copied or downloaded onto a computer.[235] Such differentiation is critical, given that only physical goods fall within the regulatory governance of the UK Sales of Goods Act (SGA),[236] which puts the burden on software vendors to ensure that software sold is of satisfactory quality and fitness of purpose.[237] An argument could therefore be made that software has significantly evolved since 1996, thus necessitating that the definition of software be updated to include intangibles.

D. China

No analysis of software resilience would be complete without investigating China's approach to the topic. Under the ordinary civil law of China, a "manufacturer" may be strictly liable for defects, while a mere "seller" is typically held to a fault standard.[238] A defect may exist when national law or private-industry guidelines for safe production or design have not been followed.[239] In addition, regulators are empowered to order products to be recalled for posing an "unreasonable danger" to people or property.[240] Private suspension of sales also seems to be expected in defects cases.[241]

---

228. *See id.* at § 4 (Amendment of section 3).

229. *Id.* at § 14 (Deletion of Sections 17 and 18 and insertion of new Part 3A, 16I).

230. *Id.* at § 14 (Part 3A).

231. *Id.* at § 18 (New section 29A).

232. *Id.* at § 20 (New sections 37A to 37D).

233. (1996) 4 All E.R. 481 (Eng.).

234. Joseph Lee & Vere Marie Khan, *Blockchain and Smart Contract for Peer-to-Peer Energy Trading Platform: Legal Obstacles and Regulatory Solutions*, 19 UIC REV. INTELL. PROP. L. 285, 299 (2020).

235. *See Division XIX Product Liability, D Liability Under the Consumer Protection Act 1987, 1 Meaning of "Product"*, BUTTERWORTHS PERS. INJ. LITIG. SERV., at 154 (Sept. 17, 2018).

236. *Id.*

237. Cyril Chua, *Limitation of Liability Clauses in IT Agreements*, L. GAZETTE, https://v1.lawgazette.com.sg/2003-8/Aug03-feature2.htm [https://perma.cc/2D7K-PXP4] (referencing Section 14 of the UK Sales of Goods Act).

238. Yue Dai, Zhenghao Li & Xiaokun Yuan, *Product Liability & Safety 2024 - China*, CHAMBERS & PARTNERS (May 23, 2024), https://practiceguides.chambers.com/practice-guides/product-liability-safety-2024/china [https://perma.cc/SPB3-TFS6].

239. *See id.*

240. *Id.*

241. *Id.*

In actions for damages, unreasonable danger appears to be a foreseeability standard in practice, based on a risk attendant to ordinary use or use not contrary to explicit manufacturer instructions.[242] As in many other countries, there are also specific laws for food safety, medicines, medical devices, automobiles, and consumer product safety.[243] A mental state of purpose or knowledge in sales of nonconforming or misbranded products, as with counterfeit medicines, may lead to criminal liability in cases where death or serious personal injury or even serious damage to buildings or other products occurs.[244]

China's encouragement of greater cybersecurity has normative and technical aspects. Like the Constitution and other statutes, one aim is to minimize risks to the Chinese Communist Party's government.[245] According to the country's 2021–2025 plan, China's agenda in the digital realm includes a completed 5G infrastructure, comprehensive information security including data encryption and "technical monitoring methods" for data, and "the healthy and orderly development of social media e-commerce, live streaming e-commerce, knowledge sharing, . . . industrial Internet, Internet of Vehicles, . . . [and] cloud computing . . . ."[246]

The Cybersecurity Law (CSL), passed in 2016, adopts a preventative approach based on targeting excessive risks. It promotes cybersecurity with regulatory structures, data protection, and infrastructure control/network emergency response protocols.[247] The regulatory framework aims to identify risks and place an emphasis on shielding high-priority networks from damage.[248] The CSL is an overlay on other legal and bureaucratic systems, with potential conflicts or actions at cross-purposes being one consequence.[249] The State Council promulgates rules, while the Ministry of Public Security also has a role.[250] A cybersecurity review mechanism examines whether hardware and software products are insecure, including risks involving data leaks.[251] By 2023, multinational companies were submitting their data security

---

242. *See id.*

243. *Id.*

244. *Id.*

245. *See* Rogier Creemers, *Cybersecurity Law and Regulation in China: Securing the Smart State*, 6 CHINA L. & SOC. REV. 111, 117–18 (2021).

246. *See* CENT. COMM'N FOR CYBERSECURITY & INFORMATIONALIZATION, THE 14TH FIVE-YEAR PLAN FOR NATIONAL INFORMATIZATION (Johanna Costigan & Graham Webster eds., Rogier Creemers, Hunter Dorwart, Kevin Neville & Kendra Schaefer trans., DigiChina Forum 2021), https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/ [https://perma.cc/E6X7-CGP7].

247. *See* Creemers, *supra* note 245, at 112.

248. *Id.* at 116.

249. *Id.* at 126.

250. *Id.*

251. *Id.* at 128; *see also* Data Security Law of the People's Republic of China, No. 84 (promulgated June 10, 2021, effective Sept. 1, 2021), http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html [https://perma.cc/XCZ3-23XP]; Personal Information Protection Law of the People's Republic of China, No. 91 (promulgated Aug. 20, 2021, effective Nov. 1, 2021), https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/ [https://perma.cc/J46W-UK4A]; Standard Contract for Outbound Personal

compliance programs to Chinese authorities with increasing frequency.[252] These authorities considerably enhanced the incentive to file these plans by issuing a $1.13 billion fine to ride-hailing giant Didi for a pattern of cybersecurity and data protection failings and by following this up with new penalty rules a few months later.[253]

Another area of intense activity in China is antimonopoly laws. The Antimonopoly Law of 2007 is part of a wide cultural and jurisprudential influence for the U.S. Sherman Antitrust Act.[254] The Abuse of Dominant Positions and Monopoly Agreements provisions of 2019 took the law in some new directions, arguably further harmonizing it with U.S. standards for proving illegal collusive activity and identifying permissible exercises of dominant market shares to improve "product safety" or engage in ordinary marketing or design practices.[255] The Platform Economy Monopoly guidelines of 2021 placed a spotlight on exclusionary conduct by digital platforms.[256] Finally, the Antimonopoly amendments and Unfair Competition Interpretation of the Chinese Supreme Court in 2022 could have important implications for misuse of user data by online platforms to reinforce dominant market positions, further increase concentration in a sector, or degrade service quality in terms of privacy.[257] For example, Article 22 of the 2022 amendments restricts "unreasonable" conditionality of dominant firms when they offer products or services to the public, as well as unjustifiable refusals to offer a quality service or a fair and nondiscriminatory price. Might a proprietor of a dominant app be liable for taking advantage of the dependency of business users on

---

Data, No. 13 (2023) (China), https://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm [https://perma.cc/2JMG-9MAD].

252. *See, e.g.*, Lorna Chen & Jieni Ji, *How Cos. Can Comply with China's Cybersecurity Rules*, LAW360 (Aug. 11, 2023), https://www.law360.co.uk/articles/1706985/how-cos-can-comply-with-china-s-cybersecurity-rules [https://perma.cc/EEA9-2MJ5].

253. *Id.*

254. *See, e.g.*, Anu Bradford, Adam Chilton, Katerina Linos & Alex Weaver, *The Global Dominance of European Competition Law Over American Antitrust Law*, 16 J. EMPIRICAL L. STUD. 731 (2019) (noting how China's antimonopoly law mimics Europe's); Antonios Platsas, *Comparing and Contrasting the EU and the US Approach in Competition Law: So Close but So Far*, EU ANTITRUST: HOT TOPICS & NEXT STEPS 481, 485, 487–88 (2022), https://cris.brighton.ac.uk/ws/portalfiles/portal/32797163/AE_Platsas_Comparing_and_Contrasting_the_EU_and_the_US_Approach_in_Competition_Law.pdf [https://perma.cc/ZVH9-GGHM] (noting that Europe's key antitrust provisions, Articles 101 and 102 TFEU, align with sections 1 and 2 of the Sherman Antitrust Act of 1890).

255. Sébastien Evrard, Emily Seo & Bonnie Tong, *Antitrust in China - 2019 Year in Review*, GIBSON DUNN (Feb. 10, 2020), https://www.gibsondunn.com/wp-content/uploads/2020/02/antitrust-in-china-2019-year-in-review.pdf [https://perma.cc/WU7U-66SW].

256. *See* PwC China, *China Issues - New Anti-Monopoly Guidelines Targeting Online Platform Sector* (2021), https://www.tiangandpartners.com/en/china-issues-new-anti-monopoly-guidelines-targeting-online-platform-sector-feb2021.pdf [https://perma.cc/HSQ7-45D7].

257. *Cf.* Jing Wang, *Competition Neutrality in Courts: Can China's Anti-Monopoly Law 2022 Ensure the Supremacy of Competition Law in Antitrust Private Litigation Involving State-Owned Enterprises*, 15 GLOB. COMPETITION LITIG. REV. 132 (2022).

their services to exploit them with purposeful or reckless vulnerabilities in the app?[258] The Chinese Supreme Court has promulgated rules for competition indicating that malicious actions like redirecting traffic or interfering with competitors' or users' intended courses of action may be unfair and illegal.[259] Similarly, its rules suggest that exploiting unwitting business users' data by creating or maintaining insecure data stores or interfaces could be a form of unfair competition.[260]

E. India

Like other Asian countries including China, India is working to capitalize on the digital revolution in an effort to influence the country's fiscal development.[261] AI technologies have matriculated into numerous Indian industries including healthcare, technology, the labor force, and education.[262] The country has invested in agricultural robotic technologies (agribots) to weed, fertilize, and harvest crops.[263] To help mitigate roadway congestion and reduce greenhouse gases, India's government has proposed the use of semi-autonomous vehicles.[264] The country's Supreme Court is working to actively incorporate and use AI in its judicial processes.[265] However, AI remains an emergent field in India, resulting in its

---

258. *Id.* at 7 n.38. Similarly, the acceptance of e-commerce manipulation cases by the High People's Court of Beijing and the State Administration for Market Regulation in 2023 may signal a shift to condemnation of practices including self-preferencing by powerful platforms. *See* Sophie Yu, Li Qiaoyi, Casey Hall, *JD.com Wins Antimonopoly Lawsuit Against Alibaba*, REUTERS (Dec. 29, 2023), https://www.reuters.com/technology/jdcom-wins-antimonopoly-lawsuit-against-alibaba-2023-12-29/ [https://perma.cc/3KE2-V5QP]; Han Ye, Lushen Hong, Yue Liu & Kuan Chen, *China: Evolving Data Monopoly Regulation Reflects Growing Focus on Anticompetitive Conduct*, GLOB. COMPETITION REV. (May 17, 2024), https://globalcompetitionreview.com/guide/data-antitrust-guide/first-edition/article/china-evolving-data-monopoly-regulation-reflects-growing-focus-anticompetitive-conduct [https://perma.cc/FYE3-QERK].

259. *See, e.g.*, Jan Holthuis, *Chinese Supreme Court Issued New Rules for Anti-unfair Competition Disputes*, BUREN LEGAL (May 23, 2022), https://www.burenlegal.com/en/news/chinese-supreme-court-issued-new-rules-anti-unfair-competition-disputes [https://perma.cc/6WM6-JMZ9].

260. *See id.*

261. Divij Joshi, *AI Governance in India – Law, Policy and Political Economy*, 10 COMMC'N RSCH. & PRAC. 328, 329 (2024), https://www.tandfonline.com/doi/epdf/10.1080/22041451.2024.2346428 [https://perma.cc/8EY6-PUNU].

262. Rahul Kapoor & Theresa T. Kalathil, *AI Regulation in India: Current State and Future Perspectives*, MORGAN LEWIS (Jan. 26, 2024), https://www.morganlewis.com/blogs/sourcingatmorganlewis/2024/01/ai-regulation-in-india-current-state-and-future-perspectives [https://perma.cc/4BES-TEXD].

263. Scott J. Shackelford, Isak Nti Asare, Rachel Dockery, AnjanetteH. Raymond & Alexandra Sergueeva, *Should We Trust a Black Box to Safeguard Human Rights? A Comparative Analysis of AI Governance*, 26 UCLA J. INT'L. & FOR. AFF. 11, 75–76 (2022).

264. *Id.* at 76.

265. Vikas Mahendra & Arunima Athavale, *Use and Regulation of AI in Dispute Resolution: Focus on the United Kingdom, Singapore and India*, 18 DISP. RESOL. INT'L 5, 5, 20–25 (2024).

government being somewhat reluctant to regulate it.[266] Still, various initiatives have been introduced to enhance the successful deployment of AI technologies.[267]

For example, because India was initially slow to engage in the rapidly evolving AI revolution,[268] its government asked the National Institution for Transforming India ("NITI Aayog")—the country's lead policy think tank[269]—to establish a national strategy for AI expansion in 2018.[270] Entitled #AIFORALL, the published report encouraged technological advancement, while positioning India to more competitively engage in global Research and Development ("R&D").[271] NITI Aayog's report focused on five main Indian sectors—healthcare, agriculture, education, smart cities and infrastructure, and smart mobility and transportation—that derive the greatest benefit from emerging AI technologies.[272] In addition, the report identified five barriers to large-scale AI deployment in India, including lack of broad-based AI experience, absence of enabling data ecosystems and access to intelligent data, high resource costs and low awareness for AI adoption, privacy and security issues, and a lack in any collateral approach to adopting and applying AI.[273] Ultimately, NITI Aayog's goal was to identify mechanisms that might encourage technological responsibility, while harnessing technological advancements and protecting Indian citizens.[274]

In February 2021, NITI Aayog released Part 1 of an Approach Document to #AIFORALL that explored two major considerations for the responsible deployment of AI: (1) ethical and (2) managerial considerations.[275] Titled *Responsible AI*, Part 1 breaks ethical considerations into two groupings—systems considerations and societal considerations.[276] Systems considerations focuses on AI design choices and deployment processes that could impact stakeholders—including private, public,

---

266. *Id.* at 20–24 ("The absence of regulation [in India] appears to be a conscious decision taken to encourage more widespread use of AI.").

267. Kapoor & Kalathil, *supra* note 262.

268. Utkarsh Amitabh, *India Is a Latecomer to AI. Here's How It Plans to Catch Up*, WORLD ECON. FORUM (Jun. 14, 2018), https://www.weforum.org/agenda/2018/06/india-latecomer-artificial-intelligence-niti-aayog/ [https://perma.cc/3QCB-GL5E].

269. *See NITI Aayog*, NAT. PORTAL OF INDIA, https://www.niti.gov.in/ [https://perma.cc/VFZ2-LGMG].

270. NITI AAYOG, NATIONAL STRATEGY FOR ARTIFICIAL INTELLIGENCE #AIFORALL 5 (2018), https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf [https://perma.cc/XZM6-H2FX].

271. *Id.* at 50 (noting India's historic lag in AI research); *see also* Amitabh, *supra* note 268 ("[#AIFORALL] encourages the development of technology to solve India's unique set of challenges and explores opportunities to leapfrog and build the foundational R&D capability necessary for global competitiveness.").

272. NITI AAYOG, *supra* note 270, at 7.

273. *Id.*

274. NITI AAYOG, RESPONSIBLE AI #AIFORALL: APPROACH DOCUMENT FOR INDIA, PART 1 – PRINCIPLES FOR RESPONSIBLE AI 2 (2021), https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf [https://perma.cc/DA5D-SQFC] (referencing recommendations established in the 2018 #AIFORALL strategy report).

275. *See generally id.*

276. *Id.* at 3.

research institutes, and governmental bodies[277]—while societal considerations focuses on the ethical challenges and risks that AI solutions may have on society, like employment and job creation.[278]

To responsibly manage AI systems, Part 1 of the Approach Document establishes principles based on India's accepted value system, and internationally-recognized global standards,[279] including the right to equality, right against discrimination, right to life and healthcare, right to privacy, economic equality, and transparency and accountability.[280] Although Part 1 does not go so far as to provide a legal or regulatory approach to managing AI systems,[281] it supports the position that finding common acceptable behaviors across relevant stakeholders, and clarifying the application of existing policies and regulations through the creation of a guiding framework, is critical.[282]

In August 2021, India published Part 2 of the Approach Document, which focuses on operationalizing principles for responsible AI.[283] It identifies necessary actions to deploy responsible AI by the government, private sector, and research institutions, to include designing regulatory and policy interventions,[284] building awareness and capacity,[285] designing procurement strategies,[286] facilitating operationalization of a trusted responsible AI ecosystem,[287] incentivizing ethics-by-design,[288] and highlighting compliance mechanisms and responsible AI practices.[289]

Two years later, the Indian government enacted the Digital Personal Data Protection Act (DPDA),[290] which balances individual data privacy rights with third parties' need to process data for lawful purposes.[291] The DPDA applies to digital personal data processed within India's territory but does not apply to personal data that is either not digitized, or is otherwise offline.[292] Individual consent and notice

277. *Id.* at 2.
278. *Id.* at 3.
279. *Id.* at 38.
280. *Id.* at 39–40.
281. *Id.* at 30–31 (discussing various global approaches to establishing an AI framework, including the EU's *Ethics Guidelines for Trustworthy AI*, Singapore's *Model AI Governance Framework*, and the United States' *Principles for the Stewardship of AI Applications*).
282. *Id.* at 30.
283. *See* NITI AAYOG, RESPONSIBLE AI #AIFORALL, APPROACH DOCUMENT FOR INDIA, PART 2 – OPERATIONALIZING PRINCIPLES FOR RESPONSIBLE AI (2021), https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf [https://perma.cc/V9YJ-R4TL].
284. *Id.* at 12–18.
285. *Id.* at 18–20.
286. *Id.* at 20.
287. *Id.* at 20–24.
288. *Id.* at 27.
289. *Id.* at 27–30.
290. The Digital Personal Data Protection Bill, 2023, Bill No. 113 of 2023 (Aug. 11, 2023).
291. Chris Brook, *What Is India's Digital Personal Data Protection (DPDP) Act? Rights, Responsibilities & Everything You Need to Know*, FORTRA (July 24, 2024), https://www.digitalguardian.com/blog/what-indias-digital-personal-data-protection-dpdp-act-rights-responsibilities-everything-you [https://perma.cc/87L5-9NPA].
292. *Id.*

are critical features of the law, although the DPDA offers some exemptions in certain cases.[293]

In addition to the above efforts, India's Ministry of Electronics & Information Technology has created four committees to further the eventual possibility of an AI Policy Framework.[294] These Committees include (1) Platforms and Data for AI, (2) Leveraging AI for identifying National Missions in Key Sectors, (3) Mapping Technological Capabilities, and (4) Cyber Security, Safety, Legal and Ethical Issues.[295] India is also a member of the Global Partnership on Artificial Intelligence (GPAI), where experts present works on responsible AI, data governance, and future innovation and commercialization.[296]

F. Summary

Part III has underscored significant areas of convergence and divergence across leading global cyber powers. Table 2 compares our key findings, which are unpacked further in Part IV.

---

293. *See* Anirudh Burman, *Understanding India's New Data Protection Law*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Oct. 3, 2023), https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en [https://perma.cc/TM4Y-J5SJ] (discussing exemptions to consent and notice include instances of data processing used to enforce legal rights or claims, personal data processing used by courts and tribunals, and circumstances where non-Indian residents' personal data is processed within India).

294. *See* Ministry of Electronics & Information Technology, Office Memorandum, Constitution of Four Committees for Promoting Artificial Intelligence (AI) Initiatives and Developing a Policy Framework, No. 4(8)/2017-ITEA (July 2, 2018) (India).

295. *Id.*

296. Kapoor & Kalathil, *supra* note 262.

Table 2: Software and Products Liability Comparison

EU	UK	Singapore	China	India
The EU Products Liability Directive (PLD) recently expanded the definitions of *"product"* to include software, and *"defect"* to include cybersecurity vulnerabilities. It also mandates that all software on the market must meet users' expected security standards. The proposed Cyber Resilience Act (CRA) requires manufacturers to have known vulnerabilities patched prior to market introduction and maintain security updates for a minimum of five years.	The Products Liability Directive (PLD) has been interpreted to account for software in recent years. The PLD enables consumers to seek compensation for harm caused by proven defects in software. This liability extends to other products if the defective software is essential to their functionality. It remains unclear whether software vulnerabilities exploited by attackers can be legally defined as "defects."	The Model AI Governance Framework emphasizes accountability, transparency, and overall responsibility in creating AI models. This framework focuses on fostering security and trust during software development, testing, and reporting. While not legally required, it strongly encourages stakeholders to prioritize the safety of AI software before introducing products to the market.	Information on China's software liability policies is limited. Unlike other cyber powers, Chinese law holds manufacturers strictly liable for product defects, with sellers only held to a fault standard. Currently, antimonopoly policies imply that exploiting software vulnerabilities may be considered unfair competition and deemed illegal.	Despite the emphasis on creating guidelines and principles for ethical AI use, India currently lacks a specific legal framework for software products liability.

IV. IMPLICATIONS FOR POLICYMAKERS

What lessons does this study hold for U.S. policymakers and their counterparts around the world as they seek to build resilience in the software ecosystem? A natural first question is whether Europe has taken a more active regulatory approach because its technology sector is much smaller. While having a smaller technology sector in Europe inevitably means that there are different political economy dynamics, including lower returns to lobbying, there is nonetheless a growing recognition that the absence of clearer guidelines and regulations is a lose-lose situation in the long run. For instance, a voluminous body of empirical literature documents a rise in concentration and market power, particularly among digital intermediaries, and that could be attributed to lax and ambiguous guidelines.[297] Only recently has the U.S. Securities and Exchange Commission introduced guidance requiring that public companies report data breaches four business days after the incident is determined material.[298]

The EU's efforts to extend products liability law to software, adopt a secure by design approach similar to that called for in the 2023 U.S. National Cybersecurity Strategy, and enhance transparency and accountability across the digital ecosystem have solidified its place as a global leader in tech governance. Several of these steps could be taken in the U.S. context at once—perhaps as part of the proposed American Privacy Rights Act, which would offer enhanced powers to the Federal Trade Commission to investigate deceptive or defective products and establish baseline privacy and cybersecurity expectations for American consumers.

At the highest level, if a products liability approach in the U.S. context is to be successful, Congress would need to introduce a package of reforms that would address various barriers to recovery, including the economic loss doctrine and the enforcement of liability waivers.[299] Moreover, the array of EU initiatives surveyed above still give rise to uncertainty, such as a potential cap of 70 million euros on all claims for a specific defective item. And costs should not be underestimated—one U.S. House of Representatives Oversight and Accountability Committee report claimed 20.4 to 46.4 billion euros in new compliance and operation costs introduced by the DSA and the GDPR. Still, such estimates should be weighed against the staggering economic harm introduced by software vulnerabilities discussed above.[300]

In 2025, these costs came to the fore with a Federal Communications Commission (FCC) letter and White House memorandum on large fines against U.S. companies.

---

297. *See* Christos A. Makridis & Joel Thayer, *The Big Tech Antitrust Paradox: A Reevaluation of the Consumer Welfare Standard for Digital Markets*, 27 STAN. TECH. L. REV. 71 (2024).

298. Sanjay Bhakta, *How Businesses Should Respond to the SEC's Cybersecurity Disclosure Rules*, REUTERS (Apr, 16, 2024), https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/cybersecurity-disclosure-rules/ [https://perma.cc/9SMF-3QAX].

299. Sharma & Zipursky, *supra* note 10.

300. Nadia Scharf, *Can the EU's Digital Services Act Inspire US Tech Regulation*?, NATION (Jan. 11, 2024), https://www.thenation.com/article/politics/european-union-digital-services-act-us-tech-regulation/ [https://perma.cc/Z9KE-2CUR].

The White House characterized the fines levied against or held over the heads of American business executives as "disproportionate" and "extortion."[301] The response would be tariffs, which followed on April 2, 2025, triggering stock market corrections, and occasionally halts to trading to prevent a free fall in markets exposed to trade risk.[302] The Chamber of Progress, a lobbying group bringing together Apple, Google, and Meta, among other firms, echoed the White House's red flag to Europe on fines.[303] The FCC Chair, Brendan Carr, conveyed the administration's resolve to combat censorship by DSA fines, and he requested information from affected platforms by early March 2025 regarding "geofencing" or other plans to safeguard freedom of speech for U.S. social media users, despite Europe's mandate that "trusted flaggers" be allowed to fast-track requests to delete posts insulting alive or dead persons, or religious beliefs.[304] Executives at Meta and X have been particularly outspoken against DSA fines as a mechanism to promote "censorship."[305] Amazon

---

301. *See* Ellen O'Regan, *Is a Billion Dollar Tech Fine Really a Tariff in Disguise?*, POLITICO (Mar. 13, 2025), https://www.politico.com/newsletters/digital-future-daily/2025/03/13/is-a-billion-dollar-tech-fine-really-a-tariff-in-disguise-00229088 [https://perma.cc/UQ6E-AC8D]; Gian Volpicelli & Alberto Nardelli, *Trump Free Speech Attack on Europe Sets Up Big Tech Fight*, BLOOMBERG L. (Feb. 21, 2025), https://www.bloomberg.com/news/articles/2025-02-21/trump-free-speech-attack-on-europe-sets-up-big-tech-fight [https://perma.cc/4DKJ-BU6P]; *Defending American Companies and Innovators from Overseas Extortion and Unfair Fines and Penalties*, THE WHITE HOUSE (Feb. 21, 2025), https://www.whitehouse.gov/presidential-actions/2025/02/defending-american-companies-and-innovators-from-overseas-extortion-and-unfair-fines-and-penalties/ [https://perma.cc/7C9Y-AG72].

302. *See* Elaine Kurtenbach, Stan Choe & David McHugh, *US Stocks Dip After Careening Through a Manic Day Following Trump's Latest Tariff Threat*, AP NEWS, https://apnews.com/article/stocks-markets-nikkei-tariffs-trump-76d0de278a6cad291ace624a74a6a1b6 [https://perma.cc/7DE7-3GMV] (Apr. 7, 2025, 6:11 PM); *Poland's Bourse Halts Trading on All Markets*, REUTERS (Apr. 7, 2025, 10:09 AM), https://www.reuters.com/markets/europe/polands-bourse-halts-trading-all-markets-2025-04-07/ [https://perma.cc/Q5TF-S4X5].

303. *See* Volpicelli & Nardelli, *supra* note 301.

304. *See* Letter from Brendan Carr, Chair, FCC, to Ms. and Messrs. Pichai, Jassy, Cook, Rolansky, Zuckerberg, Nadella, Ready, Spiegel, Iskander, and Yaccarino (Feb. 26, 2025), https://www.fcc.gov/sites/default/files/Chairman-Letter-to-Big-Tech-on-Digital-Services-Act.pdf [https://perma.cc/ZL4E-BBEX] ("Amidst this European overreach, President Trump has made clear that the United States will defend American companies from discriminatory laws and foreign regulatory regimes that wrongly burden our businesses."); *id.* at 2–3 ("The DSA undermines U.S. companies' ability to adhere to First Amendment principles by requiring them to censor, monitor, and report on users' speech. . . . [G]eofencing has been proposed as a potential solution—bifurcating your platforms into one consistent with EU law and a separate one for free speech.").

305. *See* Gian Volpicelli, *Meta Is Ready to Bring Trump into Play in Fight Against EU Rules*, BLOOMBERG L. (Feb. 16, 2025, 9:28 AM), https://www.bloomberglaw.com/product/blaw/bloombergterminalnews/bloomberg-terminal-news/SRRU6DDWX2PS [https://perma.cc/AZ3J-ZHXY]; *see also* AFP, *EU Deepens Probe into X After Musk Outbursts*, FRANCE24 (Jan. 17, 2025, 1:09 PM), https://www.france24.com/en/live-

and Meta, confronting massive European fines as well as severe U.S. legal problems involving the Department of Justice, have offered lucrative deals to persons and entities close to the White House.[306] Vice President JD Vance also warned Europe against censorship of AI, in the same month as the White House memorandum on huge fines over social media speech, with members of the European Parliament responding that they opposed relaxing AI Act requirements and wanted to shield "democracy" from the risk of AI promoting "extreme political positions, . . . policies that undermine model reliability, . . . foreign interference or election manipulation, [or] discrimination," and a European commissioner reaffirming her view that AI must be "fair, safe and democratic."[307]

The costs of the GDPR and the DSA could increase dramatically with the introduction of private enforcement by class action lawsuits in Europe.[308] Traditionally, the absence of vigorous private enforcement on a U.S. model has tempered the impact of large potential fines for breaching European laws.[309] In 2025, a European directive regarding qualified organizations asserting the legal interests of European consumers in collective actions had been "approved" in nearly all 27 European Union nations.[310] This ramp-up in GDPR litigation might be turbocharged by reducing the independence and bipartisanship of a board that monitors alleged legal limits on mass surveillance; this board is relied on by the U.S.-EU Transatlantic Data Privacy Framework to overcome the inadequacy of U.S. privacy standards with

---

news/20250117-eu-deepens-probe-into-x-after-musk-outbursts [https://perma.cc/AF5U-BTE7].

306. *See* Foo Yun Chee, *Amazon Loses Court Fight Against Record $812 Mln Luxembourg Privacy Fine*, REUTERS (Mar. 19, 2025, 2:44 PM), https://www.reuters.com/technology/amazon-loses-court-fight-against-record-812-mln-luxembourg-privacy-fine-2025-03-19/ [https://perma.cc/UQ6E-AC8D]; Jake Tapper (@jaketapper), *WSJ: Trumps Rake in Millions After Presidential Win*, INSTAGRAM (Feb. 14, 2025), https://www.instagram.com/jaketapper/reel/DGEeRNlxkNv/ [https://perma.cc/Q9M4-4D6J]; *cf.* Sophia Cai, *TikTok Celebrates Trump Inauguration, Over and Over*, POLITICO (Jan. 20, 2025, 8:31 AM), https://www.politico.com/live-updates/2025/01/20/donald-trump-inauguration-day-news-updates-analysis/tiktok-fetes-trump-all-weekend-00199235 [https://perma.cc/4CRK-FLP8]; Samuel Stolton, *TikTok Faces Fine Over €500 Million for EU-China Data Export*, BLOOMBERG L. (Apr. 3, 2025, 12:22 PM), https://news.bloomberglaw.com/business-and-practice/tiktok-faces-fine-over-500-million-for-eu-data-sent-to-china [https://perma.cc/ASA9-A7UQ].

307. Melissa Heikkilä & Barbara Moens, *EU Lawmakers Warn Against 'Dangerous' Moves to Water Down AI Rules*, FIN. TIMES (Mar. 25, 2025, https://www.ft.com/content/9051af42-ce3f-4de1-9e68-4e0c1d1de5b5 [https://perma.cc/Z6D8-FKYW].

308. *See* Directive (EU) 2020/1828 of the European Parliament and of the Council 25 November 2020 on Representative Actions for the Protection of the Collective Interests of Consumers and Repealing Directive 2009/22/EC, 2020 O.J. (L 409) 1; Cassandre Coyer, *EU Privacy Watchdog Noyb Primed to Pursue US-Style Class Actions*, BLOOMBERG L. (Dec. 16, 2024, 4:52 AM), https://news.bloomberglaw.com/privacy-and-data-security/eu-privacy-watchdog-noyb-primed-to-pursue-us-style-class-actions [https://perma.cc/R2KC-YE9R].

309. *See* Karl Wörle & Oskar Josef Gstrein, *Collective Data Protection Litigation: A Comparative Analysis of EU Representative Actions and US Class Actions Enforcing Data Protection Rights*, 11 EUR. J. COMPAR. L. & GOVERNANCE 275, 278–79, 286–87 (2024).

310. *See* Coyer, *supra* note 308.

respect to the export of European's personal data, and a finding of its inadequacy—and that of U.S. law as a result—could limit EU access to, or increase the liability of, services like WhatsApp, Instagram, Facebook, X, Amazon Web Services, Microsoft, Apple, and Google.[311]

Additional casualties of treating software as a product and imposing secure-by-design as a norm might be freedoms of expression and consumer choice in digital services markets. Critics of the AI Act, the GDPR, the DSA, and statutes like the Kids Online Safety Act echo the concerns of some courts that declined to treat books, music, or video games as "products" in their information-conveying, expressive capacity or markets. In the United States, tort and products-liability law faced a long and uneven road to judicial recognition of exemptions or First Amendment heightened-intent requirements. This trend extended even to intellectual property law, where courts converged on pleading and proof standards involving a reckless or explicitly misleading effort to fool consumers, immunizing good-faith creative works that happen to confuse some people about endorsement or sponsorship of the works by brands or celebrities.

A best-case scenario would be for policymakers on both sides of the Atlantic, and beyond, to come together and find common ground to encourage the convergence of baseline software security expectations. This process could either be kicked off through a special event, such as a Global Responsible Software Summit modeled after recent ransomware and democracy summits or be added to an upcoming major gathering.[312] No nation is an island in cyberspace. How leading cyber powers—including the EU and the United States—approach the issue of software liability will make worldwide ripples, which, depending on how these interventions are crafted, could turn into a tsunami.

There is a certain convergence or transplantation process among laws regulating insecure products, including products containing embedded software and standalone software, platforms, and digital services.[313] Given that many contemporary product and software markets are multinational, harmonization of liability standards might promise some benefits or efficiencies. Companies confronting diverse laws may benefit from more efficient compliance efforts and reduced costs, and consumers living in pre-harmonized legal regimes with inadequate deterrence of or

---

311. *See* Mike Masnick, *Trump's PCLOB Purge Risks Banning Meta, ExTwitter, Google, and Even Truth Social from Europe*, TECHDIRT (Jan. 27, 2025, 12:36 PM), https://www.techdirt.com/2025/01/27/trumps-pclob-purge-risks-banning-meta-extwitter-google-and-even-truth-social-from-europe/ [https://perma.cc/B7A2-5FVH] (quoting Max Schrems, *US Cloud Soon Illegal? Trump Punches First Hole in EU-US Data Deal*, NOYB (Jan. 23, 2025), https://noyb.eu/en/us-cloud-soon-illegal-trump-punches-first-hole-eu-us-data-deal [https://perma.cc/694H-RMB9]).

312. *FACT SHEET: The Second International Counter Ransomware Initiative Summit*, THE WHITE HOUSE (Nov. 1, 2022), https://web.archive.org/web/20250108162719/https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/fact-sheet-the-second-international-counter-ransomware-initiative-summit/ [https://perma.cc/QP2W-CPEH].

313. *See, e.g.*, MATHIAS SIEMS, COMPARATIVE LAW 315–20 (3d ed., 2022) (describing debates concerning whether moving legal standards or principles from nation to nation, or "transplants"/"transplantation," is appropriate, and whether "convergence" in the content of laws should be tolerated or aimed at).

compensation for defects. On the other hand, there may be costs for companies no longer able to enjoy the cost savings associated with light-touch regimes to which they are accustomed, startups or open source/crowdfunded operations less able to comply with strict duties or obtain insurance, and consumers in places with once consumer-friendly standards that converge "downwards" or are transplanted out of existence. These issues are not merely international in character but also arise in the interstate or inter-provincial or even inter-municipal level in countries with federalism, subsidiarity, or home rule.[314]

A. Lessons for Critical Infrastructure

As was made clear by the 2024 CrowdStrike incident, large segments of critical infrastructure in the United States and around the world are dependent on software to function. In the push to "smarten" a range of core utilities, from healthcare and the grid to water and sanitation, there is a growing concern that the situation will worsen before it improves. A range of potential fixes have been suggested and reviewed in this Article. All have benefits, and drawbacks have been noted, though we argue here for an all-of-the-above approach that incorporates transparency tools like SBOM, accountability mechanisms such as CMMC 2.0, implementing secure-

---

314. Some significant issues that may divide national or state/provincial/municipal laws into categories that are more or less onerous on manufacturers or service providers include whether a producer or platform has a duty of care to help consumers protect their own privacy, whether an intrusion into personal privacy or disclosure of private facts must be "egregious" or "outrageous," whether consumer protection statutes require pleading and proving reliance on misleading claims or an intent that consumers rely on statements, whether a failure to disclose important information to consumers must be accompanied by an "intent to defraud" to constitute misrepresentation or deceit, whether an unjust enrichment claim requires pleading the absence of other ("legal"/non-"equitable") tort claims, whether a waiver of liability or "exculpatory" clause may cover recklessness or "gross negligence," and whether the peddling of consumer names or usage data to other users or to third parties constitutes a violation of "name rights" or the "right of publicity." *See, e.g.*, *In re* Facebook, Inc., Consumer Profile User Privacy Litig., 402 F. Supp. 3d 767, 796–804 (N.D. Cal. 2019) (involving various state-law claims leveled against Facebook for unauthorized sharing of user data with Facebook Platform users); *see also In re* Meta Pixel Tax Filing Cases, 724 F. Supp. 3d 987 (N.D. Cal. 2024) (holding, in case involving tracking tools installed on sites collecting sensitive personal and financial data from consumers, that Illinois consumer protection statute required pleading causation of injury by material statements of defendant, but that this requirement could be met on amendment that consumers received a communication from which material information was omitted, or under New York consumer protection statute, causation could be pled by stating that consumers actually read misleading Facebook terms of service). In the United States, there could also be regional or even federal-district divergences of approach on whether federal legislation preempts certain state-law torts; for example, Telecommunications Act of 1996, section 230 and Copyright Act, section 301 preemption frequently come up in actions for unjust enrichment, breach of an implied contract, or the right of publicity. *See, e.g.*, *In re* Jackson v. Roberts, 972 F.3d 25 (2d Cir. 2020); Montz v. Pilgrim Films & Television, Inc., 649 F.3d 975 (9th Cir. 2011); Doe 1 v. Github, Inc., No. 22-cv-06823, 2024 WL 235217 (N.D. Cal. Jan. 22, 2024).

by-design, baseline security controls, and products liability to help address the technical debt in the IoT context.

B. Lessons for Managing AI-Generated Content

Lessons learned from countries around the world, about methods to improve cybersecurity by imposing liability for insecure software on developers, will most likely require statutory action in the United States. While a federal law would be more advantageous, states have recently been in the forefront of tackling the tough problems around security and privacy, including studying and readying laws for artificial intelligence. California has been a leader in protecting the privacy and security of personal information, but its governor recently vetoed the proposed law to require AI companies to apply safety, testing, and transparency to its AI models.[315] Instead, Colorado's Artificial Intelligence Act (CAIA),[316] adopted in May 2024, is considered the first overarching law applied to AI, focusing on discrimination,[317] and is considered to be a blueprint for other states.[318] The CAIA structures AI discrimination as an unfair trade practice,[319] distinguishing between and creating different duties for those who create AI systems, developers,[320] from those who use the system, deployers.[321] It primarily applies duties of care to high-risk systems that make "consequential decision[s]"[322] about consumers.

Though the CAIA applies to AI discrimination and has a more narrow application to software security than the broader focus of this article, the statute is informative because of its application to software that causes harm, and the products liability approach that it takes.[323] A negligence duty of care is imposed upon developers to

---

315. Trân Nguyễn, *Newsom Vetoes Bill to Create AI Safety Measures, Saying It Could Hinder Innovation in California*, PBS NewsHour (Sep. 30, 2024, 2:02 PM), https://www.pbs.org/newshour/nation/newsom-vetoes-bill-to-create-ai-safety-measures-saying-it-could-hinder-innovation-in-california [https://perma.cc/4PHN-JNDR].

316. S.B. 24-205, 74th Gen. Assemb., Reg. Sess. (Colo. 2024).

317. Tatiana Rice, Keir Lamont & Jordan Francis, *The Colorado Artificial Intelligence Act*, FUTURE OF PRIVACY FORUM (July 2024), https://fpf.org/wp-content/uploads/2024/07/FPF-Legislation-Policy-Brief_-The-Colorado-AI-Act-Final.pdf [https://perma.cc/5JSK-BCJY].

318. *Employers Beware: The Rise of AI (Regulation) in Illinois, Colorado, and California*, MCGUIREWOODS (Oct. 2024), https://www.mcguirewoods.com/client-resources/alerts/2024/10/employers-beware-the-rise-of-ai-regulation-in-illinois-colorado-and-california/ [https://perma.cc/SZ7N-AEQD]. In comparison, see the Utah law that embeds AI regulation, through the Artificial Intelligence Policy Act, into its consumer protection statutory framework. S.B. 149, 66th Leg., Gen. Sess. (Utah 2024). It has also been called the first in the country to adopt an overarching consumer protection framework for AI regulation. *See* Reena R. Bajowala & Arda Goker, *Utah Enacts First AI-Focused Consumer Protection Legislation in US*, NAT'L L. REV. (Apr. 1, 2024), https://natlawreview.com/article/utah-enacts-first-ai-focused-consumer-protection-legislation-us [https://perma.cc/LCY9-5Q44].

319. Colo. Rev. Stat. § 6-1-1706(2) (2024).

320. *Id.* § 6-1-1701(1).

321. *Id.* § 6-1-1701(6).

322. *Id.* § 6-1-1701(3).

323. The argument could also be made that an AI system that causes discrimination is a

avoid algorithmic discrimination[324] when providing high risk AI systems.[325] Algorithmic discrimination is defined as when "the use of an artificial intelligence system results in an unlawful differential treatment or impact"[326] that disfavors a person because of protected characteristics.[327] The statute defines the duty of deployers as taking "reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination."[328] Importantly, a developer earns a rebuttable presumption of reasonable care if it meets the requirements set out in the statute and any promulgated rules.[329] These requirements, and the documentation, relate to data use and governance, intended use, limitations on use, discrimination evaluation and mitigation steps, and notice to deployers of the limitations of the AI system, including information about how it should or should not be utilized.[330] Furthermore, a developer is required to make accurate and current information publicly available about what reasonable steps the developer takes to address discrimination in the AI system.[331]

Deployers are held to a different negligence standard, which is explicitly pegged to employing the risk management framework issued by the National Institute of Standards and Technology (NIST).[332] Accordingly, they must have a risk management policy and program that is regularly reviewed and that reasonably addresses the identified risks. The CAIA does not include a private cause of action. The state attorney general has the authority to enforce the act.

The CAIA is a positive step toward, though does not completely satisfy, the three principles identified in this Article, which are reflected in international approaches discussed in prior Sections. It takes the products liability view of AI software developer duties by adopting negligence standards, and the rebuttable presumption in the statute provides an incentive for developers to institute stronger practices. However, the law does not provide direct remedies to injured parties, thus weakening that incentive. The imposition of a liability framework does not impose an explicit security-by-design mandate, but it promotes those principles by adopting a liability framework. The third principle, transparency, is strongly reflected in the CAIA, as it requires risk assessments and impact analyses, as well as publicly available information and notification requirements.

---

defective product.

324. § 6-1-1702(1).

325. *Id.* §§ 1701(9)(a), -1702(1).

326. *Id.* § 6-1-1701(1)(a).

327. *Id.* ("[A]ctual or perceived age, color, disability, ethnicity, genetic information, limited proficiency in the English language, national origin, race, religion, reproductive health, sex, veteran status, or other classification protected under the laws of this state or federal law.").

328. *Id.* § 6-1-1702(1).

329. *Id.* The rebuttable presumption only applies to actions taken by the Attorney General to enforce the CAIA. *Id.* § 6-1-1706(5).

330. The list of requirements is found in the subsections of section 6-1-1702(2).

331. *Id.* § 1702(4). The CAIA includes more detailed requirements that are not included in this discussion. For a summary of those requirements, see Rice et al., *supra* note 317.

332. See details in section 6-1-1703(1)–(2).

To learn from international approaches, states, or the federal government, would need to extend the products liability approach more broadly to AI security, thereby protecting vulnerable consumers and providing incentives for AI developers and designers to imbed security by design in their products. This is, notably, a departure from the recent whirlwind of AI launches from U.S. companies in a non-regulatory environment. While it may be argued that extending products liability would deter AI innovation, the risks inherent in novel AI applications are generally acknowledged by developers and beg for the imposition of reasonable duties of care to mitigate harms that cannot otherwise be avoided by consumers. Lastly, many have questioned whether transparency is an effective method of regulation, especially in the US where the onus is often placed on the individual to take enforcement action. However, for AI security in particular, transparency is key for accountability. Without understandable, or at least auditable AI, security will be impossible to achieve.

C. Recent Developments in U.S. Law of Software-Based Hazards

Legal scholars have argued that software- and internet-enabled products should create heightened "post-sale duties to warn and to fix known vulnerabilities."[333] A failure to address "software-based hazards" that came about or remained unaddressed despite a manufacturer's warnings suggests either a design defect or a violation of the tort duty to update and maintain security even after a sale.[334] Products subject to recalls in particular need to be reasonably updated.[335] Regardless of whether a software update is a regulatory or voluntary recall or not, "an obligation of reasonableness in a broader class of cases" could support "a post-sale duty to warn" or "a post-sale duty to update" on the part of those with greater knowledge of the problems and skills to solve them, abilities to correct defects, and authorities over interconnected systems or computer servers.[336] As Bryant Walker Smith points out, a manufacturer or vendor's access to data regarding "a customer's specific needs can create an obligation to meet those needs, and information about a product's actual performance can create an obligation to address newly foreseeable risks."[337] One way of preventing further harm is by using customer and product/service data to warn the public of emerging or persistent risks or vulnerabilities; another is to take advantage of ongoing or back-door access to systems to update them for security or to restrict uses that would present unreasonable dangers.[338] By analogy to Privacy

---

333. Bryan H. Choi, *Software as a Profession*, 33 HARV. J.L. & TECH. 557, 559 (2019).

334. *See* Bryant Walker Smith, *Proximity-Driven Liability*, 102 GEO. L.J. 1777, 1806–07 (2014).

335. *See id.* (citing, inter alia, H.R. REP. NO. 103-525, pt. 2, at 6 (1994)); RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 11 cmt. a (AM. L. INST. 1998)).

336. *See id.* at 1805–07 (citing, inter alia, Braniff Airways, Inc. v. Curtiss-Wright Corp., 411 F.2d 451 (2d Cir. 1969), *cert. denied*, 396 U.S. 959 (1969)); Noel v. United Aircraft Corp., 342 F.2d 232 (3d Cir. 1964); Bell Helicopter Co. v. Bradshaw, 594 S.W.2d 519 (Tex. Ct. App. 1979); Kevin R. Boyle, *The Expanding Post-Sale Duty of a Manufacturer: Does a Manufacturer Have a Duty to Retrofit Its Products?*, 38 ARIZ. L. REV. 1033, 1036 (1996)).

337. *Id.* at 1812.

338. *See id.*

and Security Plans under financial, health, or federal contracting laws, manufacturers of cyber-physical systems could even "be required to generate and update an auditable Crashworthy Code Plan that justifies how their system detects and recovers from code crash events."[339]

D. Oversight Respecting Contractual Limitations of Liability for Defective Updates

CrowdStrike warns its customers that it disclaims liability whether in contract, tort, or otherwise, for lost data, foregoing business, and reductions in revenue or profits. It recognizes that such a disclaimer or waiver may not be valid in the European Economic Area or other countries other than the "United States and Australia." Inside the United States, CrowdStrike's Terms of Use purports to limit its liability even in cases of knowing or negligent wrongdoing to no more than $100.[340] A further disclaimer warns customers not to rely on CrowdStrike to update its own software or systems to be and remain compatible and interoperable with third-party systems, even complex systems in the medical, energy, transportation, or telecommunication industries.[341]

With the FTC investigating the cloud computing and cybersecurity practices of companies engaged in the interstate and foreign commerce engaged in the United States, disclaimers of liability like that of CrowdStrike may come under greater scrutiny.[342] Questions may arise whether, as with Facebook, X (formerly Twitter), and other social media giants before them, changing and discretion-granting terms of service constitute misleading or unfair methods of competition. One possible outcome is a Facebook- or Uber-style independent audit or committee with oversight of CrowdStrike's (or other firms', like SolarWinds's) practices and marketing claims as to software updates and security.[343]

---

339. Bryan H. Choi, *Crashworthy Code*, 94 WASH. L. REV. 39, 114–15 (2019) (first citing Federal Information Security Management Act, 44 U.S.C. §§ 3541–49 (2018); then HIPAA Security Rule, 45 C.F.R. §§ 160, 164 (2013); and then Gramm-Leach-Bliley Act Safeguards Rule, 16 C.F.R. § 314 (2018)).

340. *See* Jacob Shamsian, *CrowdStrike's Terms and Conditions Say Most Customers Would Just Get a Refund Due to the Massive Outage, Cybersecurity Lawyer Says*, BUS. INSIDER (July 19, 2024, 3:33 PM), https://www.businessinsider.com/crowdstrike-terms-conditions-limits-damages-to-refund-2024-7 [https://perma.cc/L5PB-RY63]; *CrowdStrike Software Terms of Use*, *supra* note 46.

341. *See, e.g.*, *CrowdStrike Software Terms of Use*, *supra* note 46; *CrowdStrike Terms and Conditions*, CROWDSTRIKE, https://www.crowdstrike.com/terms-conditions [https://perma.cc/U6U2-BPRH].

342. *See An Inquiry into Cloud Computing Business Practices*, FTC (Mar. 22, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/inquiry-cloud-computing-business-practices-federal-trade-commission-seeking-public-comments [https://perma.cc/RJ5J-Y9C2] (asking for comments on whether there are data security risks "in the cloud," among other things); *cf.* Letter from John Hickenlooper, Senator, U.S. Senate, to Lina Khan, Chair, Fed. Trade Comm'n (Aug. 7, 2024), https://www.hickenlooper.senate.gov/wp-content/uploads/2024/08/Senator-Hickenlooper-Letter-to-FTC-re-CrowdStirke-Impersonations.pdf [https://perma.cc/F2HH-LHD4] (urging greater inquiry particularly into the CrowdStrike scandal).

343. *See* Michel Protti, *Final FTC Agreement Represents a New Level of Accountability*

In the 2024 litigation respecting the CrowdStrike debacle, Delta Airlines will be attempting to evade the disclaimers and limitations of liability it may have received.[344] Delta alleges a sort of "gross negligence" involving a lack of even "scant care," which may suffice in some jurisdictions to evade a disclaimer or limitation of liability for negligence.[345] CrowdStrike quickly replied that Delta was at least partially to blame, castigating the company's "failure to modernize its antiquated IT infrastructure," which is a common problem among victims of faulty updates or other defective software or services.[346]

CONCLUSION

The time has come to take stock of our growing dependence on software to run our firms and lives. The race to innovate and push out the next feature or killer app can lead to dire consequences for the digital ecosystem; more than any Uber Eats gift card can address. Transparency, monitoring, and accountability are vital elements to improving resilience in the software ecosystem on which we all depend. The time has come to move slowly, address the technical debt that has been amassed, and fix things.

---

for Privacy, META (Apr. 23, 2020), https://about.fb.com/news/2020/04/final-ftc-agreement [https://perma.cc/5E5Y-FZW3]; Mike Isaac & Natasha Singer, *Facebook Agrees to Extensive New Oversight as Part of $5 Billion Settlement*, N.Y. TIMES (July 24, 2019), https://www.nytimes.com/2019/07/24/technology/ftc-facebook-privacy-data.html [https://perma.cc/VYK7-EAEW]; Press Release, Federal Trade Commission, Uber Agrees to Expanded Settlement with FTC Related to Privacy, Security Claims (Apr. 12, 2018), https://www.ftc.gov/news-events/news/press-releases/2018/04/uber-agrees-expanded-settlement-ftc-related-privacy-security-claims [https://perma.cc/HR47-HCQA].

344. *See* Graig Graziosi, *Delta Sues CrowdStrike for $500 Million in Damages Caused by Massive Airline Cancelations*, INDEPENDENT (Oct. 26, 2024, 3:44 PM), https://www.the-independent.com/news/world/americas/delta-crowdstrike-lawsuit-airline-cancelations-b2636227.html [https://perma.cc/7D7Z-EGA2].

345. *See id.* ("If CrowdStrike had tested the Faulty Update on even one computer before deployment, the computer would have crashed."); *cf. In re* Facebook, Inc., Consumer Profile User Privacy Litig., 402 F. Supp. 3d 767, 796–04 (N.D. Cal. 2019).

346. Graziosi, *supra* note 344.