UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 22 | Issue 2 Article 6

12-1-2020

Too Dangerous to Exist: Holding Compromised Internet Platforms Strictly Liable Under the Doctrine of Abnormally Dangerous Activities

Jordan Glassman

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 22, ISSUE 2: DECEMBER 2020

TOO DANGEROUS TO EXIST: HOLDING COMPROMISED INTERNET PLATFORMS STRICTLY LIABLE UNDER THE DOCTRINE OF ABNORMALLY DANGEROUS ACTIVITIES

Jordan Glassman*

In July 2020, the Twitter accounts of several prominent public figures were compromised. The maximally high profile of these targets raises the possibility of severe physical, or, more likely, economic damages from the fallout of these security failures. Because compromises of this type are foreseeable and inevitable in the context of software security, and because there is no feasible avenue for seeking damages for the resulting purely economic losses, a new scheme for relief is needed. This Article proposes that the doctrine of strict liability for abnormally dangerous activities be applied to internet platforms whose inevitable compromises are situated to proximately cause catastrophic economic damages. This application of strict liability is measured against policy goals, and common-law obstacles to its adoption are discussed.

TABLE OF CONTENTS

* J.D. Candidate, University of North Carolina School of Law, 2022. The author would like to thank Alex Rutgers from the NC JOLT Board of Advisors and all of the NC JOLT editors and staff, particularly Andy Tabeling and Maddie Labovitz, for their assistance throughout the editorial process. Finally, thank you to Beth Bennett for support, editing, and encouragement.

> The true rule of law is, that the person who for his own purposes brings on his land and collects and keeps there anything likely to do mischief if it escapes, must keep it at his peril, and, if he does not do so, is prima facie answerable for all the damage which is the natural consequence of its escape.
>
> – Justice Blackburn, Court of Exchequer Chamber, 1868 in *Rylands v. Fletcher*[1]

I. INTRODUCTION

On July 15, 2020, the Twitter accounts of numerous prominent moguls, celebrities, and politicians were compromised, including those of Joe Biden, Barack Obama, Bill Gates, Elon Musk, and

[1] Rylands v. Fletcher, (1868) L.R. 3 H.L. 330, 339–40.

Kim Kardashian, among some 130 others.[2] The attackers offered to generously double the money of credulous users as part of an apparent bitcoin scam.[3]

While the compromise was quickly contained and the actual monetary damages were minimal, the maximally high profile of the targeted individuals immediately prompted speculation on the damage a more ambitious malicious actor could have wrought.[4] For example, because world leaders now routinely use Twitter to announce or criticize policy decisions, it is easy to envision a scenario wherein a forged tweet from the account of the U.S. President or the Kremlin could spark major financial market movement or even preemptive military action.[5]

---

[2] Joe Tidy & David Molloy, *Twitter Hack: 130 Accounts Targeted in Attack*, BBC (July 17, 2020), https://www.bbc.com/news/technology-53445090 [https://perma.cc/85WC-CCA3]; *see also An Update on Our Security Incident*, TWITTER (July 30, 2020, 5:45 PM) https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html [https://perma.cc/8BW9-6GN4].

[3] Rishi Iyengar, *Twitter Blames 'coordinated' Attack on its Systems for Hack of Joe Biden, Barack Obama, Bill Gates and Others*, CNN (July 16, 2020, 6:38 PM), https://www.cnn.com/2020/07/15/tech/twitter-hack-elon-musk-bill-gates/index.html [https://perma.cc/G5R7-MMEC]*; see also Who's Behind Wednesday's Epic Twitter Hack?*, KREBS ON SEC. (July 16, 2020, 5:41 PM), https://krebsonsecurity.com/2020/07/whos-behind-wednesdays-epic-twitter-hack/ [https://perma.cc/X5FX-J3D5].

[4] Casey Newton, *The Massive Twitter Hack Could be a Global Security Crisis*, VERGE (July 15, 2020, 8:27 PM), https://www.theverge.com/interface/2020/7/15/21325708/twitter-hack-global-security-crisis-nuclear-war-bitcoin-scam [https://perma.cc/HF34-873U].

[5] *See, e.g.,* HEATHER WILLIAMS & ALEXI DREW, ESCALATION BY TWEET: MANAGING THE NEW NUCLEAR DIPLOMACY 6 (2020), https://www.kcl.ac.uk/csss/assets/10957•twitterconflictreport-15july.pdf [https://perma.cc/Z2QP-PU6L]; *see also* Casey Newton, *A Catastrophe at Twitter*, INTERFACE (July 15, 2020), https://www.getrevue.co/profile/caseynewton/issues/a-catastrophe-at-twitter-263960 [https://perma.cc/8HYA-C4JU] ("After today it is no longer unthinkable, if it ever truly was, that someone take over the account of a world leader and attempt to start a nuclear war"). *Compare* Donald Trump (*@realDonaldTrump*), TWITTER, https://twitter.com/realDonaldTrump [https://perma.cc/L46W-PJS6] (last visited Sept. 13, 2020), *with* President of Russia (*@KremlinRussia*), TWITTER, https://twitter.com/KremlinRussia [https://perma.cc/Y8FE-6XEL] (last visited Sept. 13, 2020) (illustrating a particularly sharp and well-publicized contrast).

Given that many of the internet platforms[6] routinely used by powerful public figures lack any statutorily imposed security protocols, no consumer-facing internet service can be considered secure, much less perfectly so.[7] Under these circumstances, to what extent do Twitter and similar platforms assume liability for an inevitable compromise that results, in the extreme case, in catastrophic damages?

Widely used internet platforms have largely shielded themselves from liability through mass-market adhesion contracts, at least as against their own users.[8] In scenarios like the July 2020 Twitter hack, however, damages could extend beyond users that have agreed to the terms of service and instead affect third-party non-users. Historically, it has proven very difficult to hold platform providers liable for the actions of individuals committing

[6] The term "internet platform" is used loosely in this work to describe a globally and publicly accessible, cloud-based communications tool. "Dangerous internet platform" describes ones that should be subject to strict liability.

[7] *See* Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425, 425 (2008) ("History, however, suggests otherwise: the software market has failed to produce secure software."); Bruce Schneier, *The Twitter Hacks Have to Stop,* ATLANTIC (July 18, 2020), https://www.theatlantic.com/ideas/archive/2020/07/twitter-hacks-have-stop/614359/ [https://perma.cc/E8XZ-32EY]. The absence of regulation for social media platforms and most other targets for cyber criminals, is in sharp contrast with the healthcare and financial sectors, which are subject to heavyweight regulation. *See, e.g.*, *The Patchwork of Federal Data Protection Laws*, U.S. SENATE REPUBLICAN POL'Y COMM. (July 24, 2019), https://www.rpc.senate.gov/policy-papers/the-patchwork-of-federal-data-protection-laws [https://perma.cc/HFH7-ZLDX].

[8] Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L. J. 1553, 1562–63 (2005). For a typical example, see *Terms of Service*, FACEBOOK, https://www.facebook.com/terms.php [https://perma.cc/PC7W-492U] (last updated Oct. 01, 2020) ("We cannot predict when issues might arise with our Products. Accordingly, our liability shall be limited to the fullest extent permitted by applicable law, and under no circumstance will we be liable to you for any lost profits, revenues, information, or data, or consequential, special, indirect, exemplary, punitive, or incidental damages.").

torts using the providers' platforms.[9] While calls for modernizing the regulatory framework bracketing modern software operations become more frequent, the world is nevertheless stuck with the threat that these platforms now pose.[10]

Therefore, given the magnitude and urgency of the threat, certain particularly dangerous internet platforms, like Twitter, should be exposed to strict liability for abnormally dangerous activities when the platform is compromised and results in substantial damages. Much like those unwittingly living inside the blast radius of commercial demolitions operations, Americans are awash in the wake of global, ubiquitous communications tools. When misused by malicious hands, these tools could potentially unleash economic or even, in the most extreme cases, physical damages due to preemptive military action.[11] It is time for courts to reign in risks of that magnitude.[12]

This Article proposes that dangerous internet platforms should be held strictly liable for abnormally dangerous activities when a compromise occurs that results in substantial pecuniary loss to third-parties. Part II surveys current events which exemplify the scope of the dangers that a compromised platform could cause. Part III examines the potential avenues for liability in the event of such a compromise and highlights that a finding for a plaintiff is unlikely under any of the currently available strategies. Part IV

---

[9] *See* Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 339–40 (2005) ("[O]nline service providers enjoy total immunity from liability as both distributors and as publishers.").

[10] *See, e.g.*, Michael L. Rustad & Elif Kavusturan, *A Commercial Law for Software Contracting*, 76 WASH. & LEE L. REV. 775, 784–786 (2019).

[11] Schneier, *supra* note 7; *see also* Corinne Purtill, *Twitter Security Flaws Pose a Unique Threat to Nuclear Diplomacy, Experts Say*, ONEZERO (July 17, 2020), https://onezero.medium.com/twitter-security-flaws-pose-a-unique-threat-to-nuclear-diplomacy-experts-say-b509e0eb2aad [https://perma.cc/3KUD-NF8Z] ("A poorly worded tweet at the wrong time from a high-profile yet intemperate user . . . could instigate nuclear conflict. A fraudulent tweet sent by a malevolent actor determined to cause as much harm as possible could be even worse.").

[12] Schneier, *supra* note 7 ("Underspending on security, and letting society pay the eventual price, is far more profitable. I don't blame the tech companies. Their corporate mandate is to make as much money as is legally possible. Fixing this requires changes in the law, not changes in the hearts of the company's leaders.").

defines the doctrine of strict liability for abnormally dangerous activities and explores modern applications of the doctrine. Finally, Part V and the Conclusion propose that courts go beyond the proposals previously made in the literature and apply strict liability for abnormally dangerous activities to economic damages resulting from the malicious use of compromised internet platforms.

II. THE SCOPE OF DANGER FROM CYBERCRIME

The internet has become such a normalized part of American life for most that raising the specter of catastrophic damages might seem hyperbolic. Yet cyberattacks against states and state actors are commonplace.[13] Moreover, contrary to the impression that the widespread use of the technology might suggest, these attacks are a normal side effect of all networked software.[14] The damages resulting from such attacks lie on a spectrum, ranging from trivial to seismic.[15]

A. The Unceasing Drumbeat of Consequential Cyberattacks

Cyberattacks against internet-connected services involving states and state actors are routine.[16] These attacks range from "data

---

[13] *See, e.g.*, FED. BUREAU OF INVESTIGATION, 2019 INTERNET CRIME REPORT, https://pdf.ic3.gov/2019_IC3Report.pdf [https://perma.cc/Q78A-Q4QF] (last visited Oct. 3, 2020) (citing nearly 14,000 instances of "government impersonation" internet crimes in the United States in 2019, resulting in losses of more than 124 million dollars).

[14] *See* Andrey Evdokimov, *What It Takes to Be a CISO*, KASPERSKY DAILY (Oct. 25, 2018), https://www.kaspersky.com/blog/ciso-report/24288/ [https://perma.cc/QG6Z-Z87L] (surveying Chief Information Security Officers and finding that the vast majority assume that breaches are inevitable).

[15] *See, e.g.*, Robert P. Hartwig, *Cyberrisk: Threat and Opportunity*, 1, 14-17 INS. INFO. INST. (Oct. 2016), https://www.iii.org/sites/default/files/docs/pdf/cyber_risk_wp_102716-92.pdf [https://perma.cc/R3FE-NZ8S] (finding significant variation in the per-record damages resulting from data breaches across enterprises).

[16] *Significant Cyber Incidents*, CTR. FOR STRATEGIC AND INT'L STUD., https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents [https://perma.cc/AH7Q-W6N7] (last visited Sept. 15, 2020). COVID-19 has had an amplifying effect on incidents of cybercrime, causing a "significant target shift from individuals and small businesses to major corporations, governments and critical infrastructure." *INTERPOL Report*

theft and ransomware to the overtaking of systems with potentially large-scale harmful consequences."[17] The fallout from these attacks range widely, but substantial damages are not uncommon.[18]

Of the cyberattacks that are constantly in progress,[19] some small subset of them, when successful, result in substantial economic or political consequences. In addition to the July 2020 Twitter hack, recent examples of various kinds of cyberattacks with potentially nationwide ramifications include: (1) the recent ransomware attack on the global GPS device and services developer Garmin;[20] (2) the 2017 Equifax compromise resulting in a leak of nearly half of the American population's private data;[21] (3) the 2016 Mirai botnet attack, which made large portions of the internet unavailable for nearly a day for American and European

---

Shows Alarming Rate of Cyberattacks During COVID-19, INTERPOL, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 [https://perma.cc/JPQ2-QZ4H] (last visited Sept. 15, 2020).

[17] *Wild Wide Web*, WORLD ECON. F., https://reports.weforum.org/global-risks-report-2020/wild-wide-web/ [https://perma.cc/HMY2-LAH5] (last visited Sept. 15, 2020).

[18] *See* PUBLIC-PRIVATE ANALYTIC EXCH. PROGRAM, GEOPOLITICAL IMPACT ON CYBER THREATS FROM NATION-STATE ACTORS 1–2 (2019), https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf [https://perma.cc/SAX9-WTSL] (surveying notorious incidents affecting multinational corporations, banks, power plants, airports, and even Iran's nuclear power weapons development program); *see also* Madeline A. Labovitz, *Your Natural Gas is Not Cyber-Secure*, 21 N.C. J. L. & TECH. 217, 231 (describing a foreign natural gas pipeline explosion equivalent in magnitude to a nuclear weapon caused by malicious code); *see also infra* Section II.C.

[19] *See Cyberthreat Real-time Map*, KASPERSKY, https://cybermap.kaspersky.com/ [https://perma.cc/H6AC-Y67Y] (last visited Sept. 16, 2020).

[20] Dan Goodin, *Garmin's Four-Day Service Meltdown Was Caused by Ransomware*, ARS TECHNICA (July 27, 2020, 4:03 PM), https://arstechnica.com/information-technology/2020/07/garmans-four-day-service-meltdown-was-caused-by-ransomware/ [https://perma.cc/Y3WJ-RPYX].

[21] Michael Riley et al., *The Equifax Hack Has the Hallmarks of State-Sponsored Pros*, BLOOMBERG BUSINESSWEEK (Sept. 29, 2017, 1:33 PM), https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros [https://perma.cc/LGC5-CVP4].

users;[22] and (4) the notorious leaking of the Democratic National Committee's private emails.[23]

B. The Economic and Physical Damages Due to Cyberattacks

When a popular internet platform is compromised, rather than steal data, the attackers can weaponize the platform itself given untrammeled access to its facilities.[24] After considering the consequences of a diplomatic misunderstanding over Twitter, a study from King's College concluded that "social media [use by international leaders] has the potential to be a disruptive technology and exacerbate tensions during crises."[25] The authors of the study conclude that due to the United States' disproportionately extensive use of Twitter relative to other countries, while "tweets are unlikely to independently start a crisis . . . [t]here is a risk, however, that tweets can enable or accelerate an ongoing crisis."[26]

The King's College study assumes that the users are all legitimate government actors.[27] Malicious users masquerading as legitimate government actors could cause real-world damages, since government actors and other actors whose accounts have global reach are demonstrably vulnerable.[28] In 2011, the NBC

---

[22] Elie Bursztein, *Inside the Infamous Mirai IoT Botnet: A Retrospective Analysis*, CLOUDFLARE BLOG (Dec. 14, 2017), https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/ [https://perma.cc/23GA-MDU5].

[23] *See* Jack Goldsmith, *What is Old, and New, and Scary in Russia's Probable DNC Hack*, LAWFARE (July 25, 2016, 10:39 AM), https://www.lawfareblog.com/what-old-and-new-and-scary-russias-probable-dnc-hack [https://perma.cc/42KU-RU6G] ("The Russian hack of the DNC was small beans compared to the destruction of the integrity of a national election result.").

[24] The bulk of the scholarly legal commentary on so-called cybertorts refers most often to data breaches. This work assumes that the potential damages when a compromised platform is used to maliciously trade on the identities of prominent users, institutions, or states easily transcend those stemming from data breaches.

[25] Williams & Drew, *supra* note 5, at 5.

[26] *Id.* at 18.

[27] *Id.* at 6.

[28] *Who's Behind Wednesday's Epic Twitter Hack?*, HACKER NEWS, https://news.ycombinator.com/item?id=23864265 [https://perma.cc/8H5H-RTS2] (last visited Sept. 17, 2020) (illustrating a wide range of discussion on this topic from professionals in the software development industry); s*ee also* Justin (Gus)

News Twitter account was compromised and broadcast two fake tweets about a false attack on Ground Zero, the site of the 9/11 attacks in New York.[29] In 2017, a disgruntled contractor working for Twitter disabled U.S. President Donald Trump's account.[30] Twitter's own CEO, Jack Dorsey, had his personal account compromised in 2019.[31] Most recently, in September of 2020, the Prime Minister of India's Twitter account was compromised in yet another bitcoin scam.[32]

The possibility of substantial economic loss following a compromise by a malicious user is very real.[33] In 2013, the Twitter account of the Associated Press was compromised by Syrian hackers, resulting in a fake tweet about an explosion in the White House.[34] The result was a near-instantaneous 143-point plunge in the Dow Jones Industrial average.[35] While the market recovered quickly, unrecoverable market losses are not infeasible.[36]

Hurwitz, *Cyberensuring Security*, 49 CONN. L. REV. 1495, 1509 (2017) (discussing the range of motivations of attackers, including political or social purposes, even including advancing a political agenda).

[29] Elinor Mills, *NBC News Twitter Account Hacked*, CNET (Sept. 9, 2011, 3:33 PM), https://www.cnet.com/news/nbc-news-twitter-account-hacked/ [https://perma.cc/Q8GQ-AZTD].

[30] Mike Isaac & Daisuke Wakabayashi, *Twitter's Panic After Trump's Account is Deleted Caps a Rough Week*, N.Y. TIMES (Nov. 3, 2017), https://www.nytimes.com/2017/11/03/technology/trump-twitter-deleted.html [https://perma.cc/TE4Q-SHXB].

[31] Kate Conger, *Twitter C.E.O. Jack Dorsey's Account Hacked*, N.Y. TIMES (Aug. 30, 2019), https://www.nytimes.com/2019/08/30/technology/jack-dorsey-twitter-account-hacked.html [https://perma.cc/9TAU-2YCS].

[32] *Indian Prime Minister Modi Twitter Account Hacked*, BBC (Sept. 3, 2020), https://www.bbc.com/news/business-54007995 [https://perma.cc/UCT3-A6A6].

[33] *See* Geoffrey Ingersoll, *Inside the Clever Hack That Fooled the AP and Caused The DOW to Drop 150 Points*, BUS. INSIDER (Nov. 22, 2013, 4:14 PM), https://www.businessinsider.com/inside-the-ingenious-hack-that-fooled-the-ap-and-caused-the-dow-to-drop-150-points-2013-11 [https://perma.cc/4GES-NLYB].

[34] *Id.*

[35] Heidi Moore & Dan Roberts, *AP Twitter Hack Causes Panic on Wall Street and Sends Dow Plunging*, GUARDIAN (Apr. 23, 2013, 3:41 PM), https://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall [https://perma.cc/X62P-WV2L].

[36] *See* Shawn Langlois, *This Day in History: Hacked AP Tweet About White House Explosions Triggers Panic*, MARKETWATCH (Apr. 23, 2018, 2:08 PM),

Because the possibility of physical damages due to a preemptive military response is both outlandish and likely transcends what is reachable through a suit in the common law of torts, this analysis will focus on the more plausible scenario involving sustained or permanent losses in the financial markets: purely pecuniary losses.[37] Although the actual damages resulting from the July 2020 Twitter hack and the events discussed in this section fall short of catastrophic, the potential damages do not.[38] Bad actors are constantly looking for new ways to fraudulently exploit the market's response to disinformation.[39]

A plausible hypothetical: the Twitter and Facebook accounts of the U.S. Patent and Trademark Office are compromised and used to fraudulently announce a change in the length of U.S. patent terms from twenty years to seventeen years.[40] U.S. markets would likely immediately drop in response to such a predictable decline in medium-term revenues. The fraud is detected and the market recovers, but not before the attacker anonymously short-sells[41] shares of IBM, Intel, and Apple, among the largest American

---

https://www.marketwatch.com/story/this-day-in-history-hacked-ap-tweet-about-white-house-explosions-triggers-panic-2018-04-23 [https://perma.cc/2USM-YNPH].

[37] *See* Hartwig, *supra* note 15, at 14–17 (surveying the economic risk from the standpoint of the insurer).

[38] Alicia McElhaney, *Fake News Creates Real Losses*, INSTITUTIONAL INV. (Nov. 18, 2019), https://www.institutionalinvestor.com/article/b1j2ttw22xf7n6/Fake-News-Creates-Real-Losses [https://perma.cc/6S6U-ZWZF] (giving an example of a 341 billion dollar near-instantaneous market plummet due to an erroneous news report and estimating at least 39 billion dollars in annual market losses due to "the deliberate creation and sharing of false or manipulated information to harm others for personal, political, or financial gain" over the internet).

[39] *See* Jennifer DeTrani, *Short and Distort: How Companies are 'Bearing' Down on Market-Shifting Disinformation,* ABOVE THE L. (Feb. 6, 2020, 12:47 PM), https://abovethelaw.com/2020/02/short-and-distort-how-companies-are-bearing-down-on-market-shifting-disinformation/ [https://perma.cc/4JAR-A5VR].

[40] *@USPTO*, TWITTER, https://twitter.com/uspto [https://perma.cc/4KUU-5LYB] (last visited Oct. 5, 2020); *United States Patent and Trademark Office*, FACEBOOK, https://www.facebook.com/uspto.gov/ [https://perma.cc/GQ46-CHU3] (last visited Oct. 5, 2020).

[41] James Chen, *Short Selling*, INVESTOPEDIA (last updated Feb. 4, 2020), https://www.investopedia.com/terms/s/shortselling.asp [https://perma.cc/Y3HQ-M7XV].

assignees of thousands of patents.[42] Unable to locate the cybercriminal or recover from their losses, the affected financial institutions may seek financial redress against Twitter and Facebook.

C. The Inevitability of Compromise

The July 2020 Twitter hack described in the Introduction[43] was not the work of sophisticated criminal masterminds.[44] It was instead a fairly typical feat of social engineering, involving a deliberate campaign to deceive employees into granting access to internal administration systems.[45] Social engineering attacks exploit predictable tendencies of human beings that must inescapably be involved with the maintenance and operation of internet platforms.[46]

Beyond the vulnerability of human beings, perfectly secure software is a fantasy.[47] All software is susceptible to attack and, if networked, potentially exploitable by any connected person in the world.[48] While platform providers might make every effort to build and maintain secure systems, the most pragmatic among them operate their platforms as if the worst-case compromise might happen at any moment; indeed, effecting that worst case is likely the precise, active goal of malicious actors operating without

---

[42] *2019 Top 50 US Patent Assignees*, IFI CLAIMS PAT. SERVS. (Jan. 8, 2020), https://www.ificlaims.com/rankings-top-50-2019.htm [https://perma.cc/2NLJ-63TT].

[43] *Supra* Part I.

[44] Robert McMillan, *Twitter Links Hack to Phone-Based Phishing Attack*, WALL ST. J. (July 30, 2020, 11:37 PM), https://www.wsj.com/articles/twitter-links-hack-to-phone-based-phishing-attack-11596166657 [https://perma.cc/23KJ-RYWV].

[45] *Id.*

[46] *What is Social Engineering?*, KASPERSKY, https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering [https://perma.cc/U4KZ-HVU6] (last visited Sept. 16, 2020).

[47] Jane Chong, *Why Is Our Cybersecurity So Insecure?*, NEW REPUBLIC (Oct. 11, 2013), https://newrepublic.com/article/115145/us-cybersecurity-why-software-so-insecure [https://perma.cc/BMS3-G8EB].

[48] Bruce Schneier, *Should U.S. Hackers Fix Cybersecurity Holes or Exploit Them?*, ATLANTIC (May 19, 2014), https://www.theatlantic.com/technology/archive/2014/05/should-hackers-fix-cybersecurity-holes-or-exploit-them/371197/ [https://perma.cc/N6NL-4ANE]; *see also* Hurwitz, *supra* note 28, at 1501–07 (2017) (describing the challenges of building and operating secure software).

pause.[49] Among information security professionals, this type of thinking is not alarmist—it is axiomatic.[50] But despite the inevitability of compromise and harm, the available tort theories may not provide adequate—or any—relief.

III. EXISTING AVENUES FOR LIABILITY

A plaintiff damaged as the result of a malicious actor compromising and abusing an internet platform with sufficient reach to have substantial economic consequences might bring suit under a number of different causes of action but will probably not survive the defendant's motion to dismiss.[51] None of the mainstream options available for a harmed plaintiff in an internet platform case are likely to yield relief.

A. The Computer Fraud and Abuse Act

The starting point for identifying criminal and civil liability for the fallout of attacks on internet platforms is the Computer Fraud and Abuse Act ("CFAA").[52] While civil liability for compensatory damages, injunctive relief, or other equitable relief is available against the attacker, the CFAA explicitly exempts internet platform providers from civil liability under the provisions of the CFAA "for the negligent design or manufacture of computer hardware, computer software, or firmware," which would seem to at best

---

[49] Bruce Schneier, *The Security Mindset*, SCHNEIER ON SEC. (Mar. 25, 2008, 5:27 AM), https://www.schneier.com/blog/archives/2008/03/the_security_mi_1.html [https://perma.cc/YW49-N33H].

[50] *See Why Software Remains Insecure*, DANIEL MIESSLER (June 6, 2019), https://danielmiessler.com/blog/the-reason-software-remains-insecure/ [https://perma.cc/V5FU-VRA8] ("Basically, software remains vulnerable because the benefits created by insecure products far outweigh the downsides. Once that changes, software security will improve—but not a moment before."); *see also* Bruce Schneier, *Why Computers Are Insecure*, SCHNEIER ON SEC. (Nov. 1999), https://www.schneier.com/essays/archives/1999/11/why_computers_are_in.html [https://perma.cc/MS2J-FV6L] ("Security engineering involves programming Satan's computer. And Satan's computer is hard to test.").

[51] Rustad & Koenig, *supra* note 9, at 362–83 (explaining that "most cybertorts are stillborn").

[52] Russell Gribbell, *Ransomware & the Tort of Negligent Cybersecurity*, 45 N. KY. L. REV. 23, 39 (2018).

considerably narrow the window available for tort litigation under this legislation.[53]

In one roughly analogous case, a federal court granted injunctive relief under the civil liability provisions of the CFAA against a defendant fraudulently impersonating Facebook accounts to obtain credit to run hundreds of thousands of dollars' worth of unpaid advertisements.[54] However, when a criminal hacker is unavailable and liability is sought instead against the platform that facilitated the compromise, federal courts continue to interpret the civil liability provisions of the CFAA as not holding platforms liable for negligent, insecure software design.[55]

B. Contract Liability

While the Uniform Commercial Code ("U.C.C.") unambiguously identifies computer hardware as a good, the status of software, in its various forms, has proved harder to classify.[56] If software is a good under the U.C.C., then Article 2 provisions provide a substantial shield for internet platform providers in the form of warranty disclaimers and limitations on liability and remedies against users who have agreed to their terms of service.[57]

But the conception of software as a tangible good is out of sync with the ways software is most commonly used as of 2020: through "software licensing" or, most importantly to this analysis, through "software-as-a-service" ("SaaS"), an abstraction roughly synonymous with the popular term "cloud computing."[58] All of the platforms vulnerable to the type of attacks discussed *supra* are exclusively SaaS products, which is most closely analogized as a

---

[53] 18 U.S.C. § 1030; *see also* Hurwitz, *supra* note 28, at 1508 (describing how, as a practical matter, identifying or even successfully bringing suit against the attackers is often impossible due to the "multiplicity of actors and difficulties of designing secure systems").

[54] Facebook, Inc. v. Grunin, 77 F. Supp. 3d 965, 972 (N.D. Cal. 2015).

[55] *See, e.g.,* DHI Grp., Inc. v. Kent, No. H-16-1670, 2017 WL 9939568, at *11 (S.D. Tex. Apr. 27, 2017).

[56] *See* Rustad & Kavusturan, *supra* note 10, at 787–91.

[57] *See* Scott, *supra* note 7, at 436–37.

[58] *See* Rustad & Kavusturan, *supra* note 10, at 779–80.

"service offered through access contracts."[59] If software is a service, then it is governed by the common law of services and Article 2 of the U.C.C. does not apply.[60]

Nevertheless, the U.C.C. has been the de facto source of law for software contracts in the absence of a better alternative, with incoherent legal rationales.[61] Commentators are beginning to suggest revisions to the U.C.C. to cover the realities of modern cloud software, but until then, courts will operate without guidance and badly outdated contract law will continue to dominate.[62]

However, a tort action might still be available to a non-user who has not agreed to the adhesion contract presented by the platform provider.[63] In other words, even when it applies, the antiquated contract law of U.C.C. Article 2 will only protect platform providers from users who have voluntarily agreed to their terms of service and license agreements.[64] While many of the platforms of concern here have billions of users, there are still many billions who are not users, and thus many who have not signed away their rights to bring suit against the providers.[65] Despite having no contractual relationship to the platform

---

[59] *Id.* at 780; *see supra* Section II.

[60] Rustad & Kavusturan, *supra* note 10, at 872–73.

[61] *See id.* at 824–25 ("[I]t is a legal fiction that software licensing and cloud computing involve tangible goods.").

[62] *See generally id.* at 851–72 (proposing a new Article 2B to cover software licensing and 2C to cover cloud computing); Holly K. Towle, *Enough Already: It Is Time to Acknowledge That UCC Article 2 Does Not Apply to Software and Other Information*, 52 S. TEX. L. REV. 531, 536 (2011) (arguing that applying Article 2 to software licensing will increasingly lead to wrong results).

[63] *See* Vincent R. Johnson, *The Boundary-Line Function of the Economic Loss Rule*, 66 WASH. & LEE L. REV. 523, 553–56 (2009).

[64] *See, e.g., WECHAT - TERMS OF SERVICE*, WECHAT, https://www.wechat.com/en/service_terms.html [https://perma.cc/MD9J-FUQZ] (last updated Mar. 21, 2018) ("THESE TERMS GOVERN THE RELATIONSHIP BETWEEN YOU AND US.").

[65] *See Global Social Media Overview*, DATAREPORTAL, https://datareportal.com/social-media-users [https://perma.cc/FH48-PYYH] (last visited Oct. 4, 2020) (estimating roughly half of the world's population to be users of social media).

providers, harmed non-users will nevertheless have standing to bring suit under the usual constitutional test.[66]

C. Section 230 of the Communications Decency Act

Historically, internet platforms have been largely insulated from liability stemming from content created by their own users through Section 230 of the Communications Decency Act.[67] This broadly interpreted provision has effectively immunized internet platform providers from any liability resulting from torts committed while using their platforms by allowing the providers to self-identify as "publishers," a result upheld many times over in court.[68]

Thus, Section 230 of the Communications Decency Act would shield internet platform providers from liability under the theory that the hackers who had gained access to the compromised accounts were "information content providers" of the type specified in Section 230(c)(1).[69] While Section 230(e) explicitly exempts federal criminal acts from immunity, the status of civil actions against defendant platform providers due to the actions of third-party criminals are less clear.[70] There is substantial case law holding that providers are shielded from liability when legitimate users of services commit crimes using those services by, for

---

[66] *See, e.g.,* Valley Forge Christian Coll. v. Ams. United for Separation of Church and State, Inc., 454 U.S. 464, 472 (1982). Standing under state law might vary somewhat from these standards.

[67] 47 U.S.C. § 230; *see generally* Benjamin Volpe, *From Innovation to Abuse: Does the Internet Still Need Section 230 Immunity?*, 68 CATH. U. L. REV. 597, 601 (2019) (providing "legislative background along with an accounting of the common law history of the CDA, specifically related to § 230 immunity of internet service providers and online intermediaries").

[68] Danielle Keats Citron & Benjamin Wittes, *The Problem Isn't Just Backpage: Revising Section 230 Immunity*, 2 GEO. L. TECH. REV. 453, 458–77 (2018).

[69] *See Section 230 of the Communications Decency Act*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/cda230 [https://perma.cc/FEV2-QKL9] (last visited Oct. 4, 2020).

[70] *See* VALERIE C. BRANNON, CONG. RSCH. SERV., LSB10306, LIABILITY FOR CONTENT HOSTS: AN OVERVIEW OF THE COMMUNICATION DECENCY ACT'S SECTION 230 at 2 (2019), https://fas.org/sgp/crs/misc/LSB10306.pdf [https://perma.cc/9WPA-QVAG].

example, distributing child pornography or selling drugs.[71] How courts will interpret Section 230 where the content's author was a third party controlling a compromised account to commit a malicious act is unclear, but the history of its employment in various courts suggests that it might immunize the providers even in this context.[72]

D. Negligence

A finding of negligence will require a showing of duty, breach, causation, and damages.[73] Each of these elements present challenges for a showing of provider negligence.[74] To begin with, to date, courts have not identified a duty of care for software manufacturers to produce secure software.[75] If a duty could be identified, a test for breach would need to be embraced by courts out of the many that have been proposed.[76] Pecuniary damages might be calculable, but would likely still be filtered from claims by the economic loss rule discussed *infra*.[77]

---

[71] *See, e.g.,* Force v. Facebook, Inc., 934 F.3d 53, 64–72 (2d Cir. 2019), cert. denied, 140 S. Ct. 2761, (2020) (upholding Section 230 immunity for a social media platform providing a forum to a known terrorist organization); *see generally* Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401, 413–14 (2017) (cataloging criminal activities which have enjoyed Section 230 immunity).

[72] *See* Citron & Wittes, *supra* note 71, at 413–14 (listing particularly egregious examples of Section 230 applications); *see also* Jessica E. Easterly, *Terror in Tinseltown: Who Is Accountable When Hollywood Gets Hacked*, 66 SYRACUSE L. REV. 331, 355–60 (2016) (considering whether Section 230 shields platforms when illicit private data is stolen from users by unauthorized, malicious users). *But see* Mike Godwin, *Clarence Thomas Is Begging Someone to Sue Over Conservatives' Most-Hated Internet Law*, SLATE (Oct. 16, 2020), https://slate.com/technology/2020/10/clarence-thomas-section-230-cda-content-moderation.html [https://perma.cc/D7NU-S5DV].

[73] 65 C.J.S. *Negligence* § 19 (2020).

[74] Scott, *supra* note 7, at 442.

[75] *See* Rustad & Koenig, *supra* note 8*,* at 1567.

[76] Scott, *supra* note 7, at 448.

[77] *See infra*, Section V.C.3.

The most difficult element of negligence to establish in the context of an internet security breach is causation.[78] Because software is so complex, there might often be but-for causation in the sense that a coding error led to an exploit.[79] For the same reason, however, causation might be found to be too remote for a finding of proximate causation, especially if a standard of foreseeability is used.[80] Even if a security compromise is inevitable, as a question of fact left to the jury, the level of complexity in modern software systems provides ample fodder for demonstrating that the connection between the defendant's action and the plaintiff's injury is too "attenuated, remote, or freakish" to prevail.[81]

Overall, the negligence approach, which evolved around relatively simple physical events causing physical harm, is incompatible with the complexity of internet-based torts. "[T]he difficulty of imposing liability in negligence and contract models [stemming from cybersecurity failures] has effectively created a 'strict fault' regime . . . which is governed by negligence and contract law in name only [and in which] sophisticated parties pervasively externalize risk upon unsophisticated parties."[82]

The lens of negligence could also be focused on the decisions of internet platforms prior to the creation of the software that resulted in a compromise.[83] If the risk cannot be eliminated even after taking reasonable precautions—for example if a compromise is inevitable—then negligence might lie where an argument can be made that the platform providers never should have engaged in the activity in the first place.[84] However, even if it is arguably unreasonable to provide a technology like Twitter to world leaders

---

[78] *See* Rustad & Koenig, *supra* note 8, at 1602–03 ("Without a proximate cause limitation, internet security breaches could create boundless liability.").

[79] *See* Scott, *supra* note 7, at 448.

[80] *See* Rustad & Koenig, *supra* note 8, at 1601–02.

[81] *See* JOHN L. DIAMOND ET AL., UNDERSTANDING TORTS § 12.01, at 179 (6th ed. 2018).

[82] Hurwitz, *supra* note 28, at 1528.

[83] *See* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 20 cmt. b (AM. L. INST. 2010).

[84] *See id.*

and governments, the difficulty in adjudicating a claim of institutional incompetence means that a finding of no duty is the most likely outcome.[85]

E. Strict Product Liability

While the full force of strict product liability doctrine might be brought to bear if software is viewed as a product like any other,[86] courts have demonstrated an unwillingness to stretch the doctrine to include software as a general rule.[87] It is a fundamental theorem of strict product liability that the manufacturer of a defective product is best situated to bear the cost of personal injury or injury to property.[88] But courts have been mixed on the question of whether software is a product or service,[89] similar to the confusion surrounding the application of the U.C.C., discussed *supra*.[90]

Product liability suits can find purchase under a theory of garden-variety negligence when inadequate warnings or instructions or defective designs are at issue.[91] Alternatively, if the products are adequately designed but not manufactured according to specification, a finding of no-fault strict liability is possible.[92] For damages due to a software security compromise, it must be determined whether the compromise was the result of the design of

---

[85] *See id.* at § 7, cmt. f ("For example, when a plaintiff claims that it is negligent merely to engage in the activity of manufacturing a product, the competing social concerns and affected groups would be appropriate considerations for a court in deciding to adopt a no-duty rule.").

[86] RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 19 reporter's notes to cmt. d (AM. L. INST. 1998).

[87] Scott, *supra* note 7, at 469.

[88] *See* Escola v. Coca Cola Bottling Co. of Fresno, 150 P.2d 436, 440–41 (Cal. 1944) (Traynor, J., concurring).

[89] *See* Scott, *supra* note 7, at 466–67 ("While these factors may not argue in favor of finding all software to be products, they strongly favor finding software that is supposed to provide security for corporate and government computer systems to be a product for product liability purposes."); *see also* Bryan H. Choi, *Crashworthy Code*, 94 WASH. L. REV. 39, n. 142 (2019) (listing "tantalizing dicta" suggesting that software might be considered a product by courts).

[90] *See supra* Section III.B.

[91] RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 19 cmt. a (AM. L. INST. 1998).

[92] *See id.* § 2.

the software or the implementation of that design in code.[93] Distinguishing these two is likely to be highly fact-specific and complex, and thus unlikely to yield relief.[94] Having surveyed the avenues for recompense available via various contemporary theories of tort liability and finding them wanting, a novel application of the doctrine of strict liability for abnormally dangerous activities is considered next.

IV. STRICT LIABILITY FOR ABNORMALLY DANGEROUS ACTIVITIES

The lack of a clear cause of action for harmed plaintiffs in the event of catastrophic fallout from the inevitable compromise of an internet platform is alarming. Because the body of law that has grown alongside the internet has kept platform providers well-shielded from liability, some commentators have suggested a new route: the application of strict liability for these providers under a theory of abnormally dangerous activities.[95] This application, however, will stretch the doctrine well past the envelope of the contexts in which it has traditionally been applied.[96]

A. Abnormally Dangerous Activities Defined

The story of strict liability for abnormally dangerous activities ("SLADA")[97] in its modern form usually begins with the celebrated English case of *Rylands v. Fletcher*[98] from the

---

[93] *See* Scott, *supra* note 7, at 459.

[94] *See id.* at 467–71; Hurwitz, *supra* note 28, at 1523 ("Given the near impossibility of designing defect-free software, many commentators believe that it will be exceptionally difficult to successfully bring a products liability claim.").

[95] Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 277–96 (2007); Hurwitz, *supra* note 28, at 1526.

[96] Hurwitz, *supra* note 28, at 1527–28.

[97] The helpful acronym coined by Professor Boston is borrowed here. Gerald W. Boston, *Strict Liability for Abnormally Dangerous Activity: The Negligence Barrier*, 36 SAN DIEGO L. REV. 597, 598 (1999).

[98] Rylands v. Fletcher, (1868) L.R. 3 H.L. 330.

mid-nineteenth century.[99] In *Rylands*, the wealthy defendant John Rylands constructed a water reservoir over abandoned coal mine shafts that connected with the active coal mine owned by Thomas Fletcher on neighboring property.[100] Probably due to an error on the part of the builders, the partially-filled reservoir burst downwards, resulting in cascading flooding of the shafts underneath into Fletcher's adjacent mine.[101] Fletcher brought suit for negligence and the English courts of appeals ultimately decided for Fletcher, memorably articulating what would come to be known as strict liability for abnormally dangerous activities.[102] The decision from the intermediate appellate court highlighted the elements of outsized risk and foreseeability now found in the modern formulation, and the holding of the highest court is associated with the "common usage" portion of the doctrine.[103] The *Rylands* decisions are also notable in that they were an early example of common-law courts departing from the rigid, procedure-dominated writ system to a more flexible application of substantive law to a novel situation,[104] a suggestion which is again urged here.

The modern doctrine of SLADA provides an avenue for no-fault findings of liability against tortfeasors under limited circumstances.[105] In contrast with negligence law, in which the primary policy rationale is to encourage those with a legal duty to exercise reasonable care, strict liability is appropriate when the risk cannot easily be eliminated and a reduction of the risky activity is preferable.[106] The doctrine focuses on the inherent danger of certain activities, not on the inherent danger of particular materials.[107]

---

[99] *See generally* Kenneth S. Abraham, *Rylands v. Fletcher: Tort Law's Conscience*, in TORT STORIES 207, 209–10 (Robert L. Rabin & Stephen D. Sugarman eds., 2003).

[100] *Id.*

[101] *Id.* at 210.

[102] *Rylands*, L.R. 3 H.L. 330, 339–40.

[103] *See* Abraham, *supra* note 99, at 213–14.

[104] *Id.* at 214–215.

[105] *See* 57A AM. JUR. 2D *Negligence* § 385 (database updated October 2020).

[106] *See* James T. Graves, Note, *Minnesota's PCI Law: A Small Step on the Path to A Statutory Duty of Data Security Due Care*, 34 WM. MITCHELL L. REV. 1115, 1139–40 (2008).

[107] DAN B. DOBBS ET AL., THE LAW OF TORTS § 443 (2d ed. 2020).

Importantly for software security, the doctrine assumes that "a highly significant risk . . . remains . . . even when all actors exercise reasonable care."[108] Distilled to its essence, SLADA is a doctrine designed to "ensur[e] that liability for harms be assigned to parties best able to bear it."[109]

The Third Restatement offers two factors to consider when determining whether an activity is abnormally dangerous: "(1) the activity creates a foreseeable and highly significant risk of physical harm even when reasonable care is exercised by all actors; and (2) the activity is not one of common usage."[110] An activity is abnormally dangerous if it satisfies both factors and need not necessarily provide substantial value or utility.[111]

B. The Modern Scope of SLADA

The doctrine of SLADA evolved as the industrial revolution blossomed in England and America, and the trend towards requiring fault for a finding of liability was ascendant in courts.[112] As the world became blanketed with modern technologies, the potentially devastating effects of physical injury from probabilistic, catastrophic mechanical failures gave rise to a growing consciousness that a revised allocation of risk was needed, at least in some cases.[113]

Despite the historical and precedential association of SLADA with physical damages from large-scale disasters, courts have

---

[108] RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 20 cmt. b (AM. L. INST. 2010).

[109] Hurwitz, *supra* note 28, at 1525.

[110] RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 20 (AM. L. INST. 2010). This update to the Restatement reduced the SLADA factors in number from six to two but it is not unusual to see courts still referring to the Second Restatement factors. RESTATEMENT (SECOND) OF TORTS § 520 (AM. L. INST. 1977). *See, e.g.,* Navelski v. Int'l Paper Co., 771 F. App'x. 949, 952 (11th Cir. 2019).

[111] *See* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 20 cmt. k (AM. L. INST. 2010). The value to the community is subsumed by the question of common usage in the revised Restatement.

[112] *See* Joseph H. King, Jr., *A Goals-Oriented Approach to Strict Tort Liability for Abnormally Dangerous Activities*, 48 BAYLOR L. REV. 341, 344–46 (1996).

[113] *See id.*

varied widely in their applications of the doctrine to the facts presented by creative plaintiffs invoking it.[114] The risks and dangers under discussion here are novel, and the application of SLADA to the new fact patterns of the twenty-first century is not affirmatively foreclosed by statute or precedent, although there has been no clear application of the doctrine beyond the canonical fact patterns to date.[115]

For example, when a foreign bank brought suit against a domestic bank in *Dubai Islamic Bank v. Citibank*,[116] it requested the court invoke SLADA against the defendant, alleging that the defendant was "actively recruiting known financial terrorists . . . each of whom is *capable of destabilizing an entire country if not an entire region*, and providing them any service for which they are willing to pay."[117] The court rejected the plaintiff's proposal to extend the doctrine beyond the physical realm, stating that the court "does not feel it is appropriate to expand the scope of the strict liability doctrine to embrace the banking and financial issues presented here."[118]

In rejecting another scenario with roughly analogous geometry, courts have found that utilities operating physical plants as remote sources of services to the public are not examples of abnormally dangerous activities.[119] In *United States v. Southern California*

---

[114] *See, e.g.,* King v. United States, 53 F. Supp. 2d 1056 (D. Colo. 1999) (campfires); Thomalen v. Marriott Corp., 880 F. Supp. 74 (D. Mass. 1995) (fire-eating); State Farm Fire & Cas. Co. v. Mun. of Anchorage, 788 P.2d 726, 728 (Alaska 1990) (city water delivery systems); Bennett v. Mallinckrodt, Inc., 698 S.W.2d 854 (Mo. Ct. App. 1985) (radioactive emissions); King, Jr., *supra* note 112; *see also id.* at n.220 (highlighting various cases with plaintiffs that have applied a SLADA theory of liability for purely economic damages with mixed results).

[115] Choi, *supra* note 89, at 51–52.

[116] Dubai Islamic Bank v. Citibank, N.A., 126 F. Supp. 2d 659 (S.D.N.Y. 2000).

[117] *Id.* at 668 (emphasis added).

[118] *Id.* at 669.

[119] *See* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 20 reporter's notes to cmt. h (AM. L. INST. 2010). *See, e.g.,* Bickett v. Countrymark Energy Res., LLC, 250 F. Supp. 3d 309, 321–22 (W.D. Ky. 2017) (citing Ky. Utils. Co. v. Auto Crane Co., 674 S.W.2d 15, 18 (Ky. App. 1983)).

Edison Co.,[120] a private hydroelectric utility plant was the proximate cause of a major forest fire.[121] The government argued for strict liability, but the district court concluded that the "[claim that the] hydroelectric utility plant is an ultrahazardous activity conflicts with California law and is not supported by existing federal statutory or decisional law."[122]

Despite a disappointing lack of hints of modernization from recent case law, the SLADA doctrine should nevertheless be applied to abnormally dangerous activities conducted on internet platforms, even where the harms are not physical.

V. STRICT LIABILITY FOR ABNORMALLY DANGEROUS ACTIVITIES SHOULD APPLY TO DANGEROUS INTERNET PLATFORMS

SLADA should be applied to remedy economic damages resulting from the compromise of dangerous internet platforms by malicious actors. The highly significant risks of these platforms' activities are manifestly foreseeable, are not preventable even with reasonable care, and are not in common usage.[123] This section proposes a rule for the application of SLADA to this scenario and grapples with the objections that flow naturally from the history and precedent of the associated common law.

A. A Proposed SLADA Doctrine for Dangerous Internet Platforms

Professor Danielle Citron was among the first to propose the application of SLADA to "bursting cyber-reservoirs of personal data" in analogy to the infamous bursting water-reservoirs of *Rylands*.[124] But perhaps Citron did not take the metaphor far enough, for modern citizens are also "adjacent" to internet platforms with such latent power to do physical and economic damage that the metaphor can be safely extended to include them as well: "[a] third party's criminal acts are the natural

[120] United States v. S. Cal. Edison Co., 300 F. Supp. 2d 964 (E.D. Cal. 2004).
[121] *See id.* at 969–70.
[122] *Id.* at 991.
[123] *See* Hurwitz, *supra* note 28, at 1527 ("[T]he cybersecurity context arguably presents a more 'textbook case' for the use of strict liability than seen in most 'textbook cases.'").
[124] Citron, *supra* note 95, at 243–96.

consequences of maintaining information reservoirs in much the same way that flooding due to gravity or negligence naturally accompanied water reservoirs."[125]

The scenario exemplified by the July 2020 Twitter hack is somewhat different in kind: although it is similar to the leakage of confidential data in that it is due to the inevitable actions of malicious actors, Citron's "data breach" involves damages from theft or misappropriation of data, not damages due to the platform itself.[126] The torts suggested by the July 2020 Twitter hack are more akin to damages caused by a private nuisance, a cause of action that shares common roots with SLADA.[127]

Strict liability for dangerous internet platforms has been proposed by several commentators, but only in the context of data breaches.[128] But the scope and magnitude of the dangers that internet platforms now expose the world to in the worst-case scenario have quickly moved past those dangers associated with now-routine data breaches.[129]

Therefore, courts should consider carefully the observation made by Judge Posner:

> By making the actor strictly liable—by denying him in other words an excuse based on his inability to avoid accidents by being more careful—we give him an incentive, missing in a negligence regime, to experiment with methods of preventing accidents that involve not greater exertions of care, assumed to be futile, but instead relocating,

---

[125] *Id.* at 270–71. In 2020, we have arguably moved beyond "adjacent" in the sense that the negative effects can be felt regardless of where we physically are, or whether we in any sense opted-into the danger.

[126] *See id.* at 255.

[127] *See* Steven Kam, *Intel Corp. v. Hamidi: Trespass to Chattels & A Doctrine of Cyber-Nuisance*, 19 BERKELEY TECH. L.J. 427, 440 n.79 (2004) (describing the evolution of nuisance law from early strict liability doctrine).

[128] *See* Hurwitz, *supra* note 28, at 1498 n.1 (enumerating legal and industry scholarship on the subject).

[129] Williams & Drew, *supra* note 5, at 14; *see also* Danielle Jablanski, Herbert S. Lin, & Harold A. Trinkunas, *Retweets to Midnight*, *in* THREE TWEETS TO MIDNIGHT: EFFECTS OF THE GLOBAL INFORMATION ECOSYSTEM ON THE RISK OF NUCLEAR CONFLICT (Harold A. Trinkunas, Herbert Lin, & Benjamin Loehrke eds., 2020).

> changing, or reducing (perhaps to the vanishing point) the activity giving rise to the accident.[130]

SLADA should be applied against dangerous internet platforms when their activities have achieved such scale that an inevitable compromise by a malicious actor has a reasonable chance of resulting in substantial damages to third parties who are not users of the platform. Furthermore, if invoked, courts should reject any attempt to stretch the tortured interpretation of Section 230 of the Communications Decency Act even further to cover the "publications" of non-user cybercriminals.[131]

Whether SLADA applies, and in particular whether the activities of an internet platform should be considered abnormally dangerous, should be a question of law evaluated according to several factors:

(1) whether the platform has, as users, public figures or organizations;

(2) whether those users have the potential to effect significant damages by their words or acts;

(3) whether the words or acts of users of the platform are visible to the public;

(4) whether the publicly visible words or acts of users of the platform are construed to be directly attributable to the users; and

(5) whether there exists a reasonable likelihood of identifiable, substantial economic damages resulting from a presumed compromise.[132]

This application of SLADA is an extreme remedy; courts should justifiably be wary and apply it only when the risk is maximal and the specific alleged damages are reasonably

---

[130] Ind. Harbor Belt R.R. Co. v. Am. Cyanamid Co., 916 F.2d 1174, 1177 (7th Cir. 1990) (citation omitted).

[131] *See, e.g.,* Citron & Wittes, *supra* note 71, at 415–18 (suggesting that courts adopt a narrower reading of the statute and limit its application to actors operating in good faith).

[132] Platforms meeting criteria (1) through (4) are "dangerous internet platforms." Evaluation of (5) gives rise to the cause of action for particularly situated plaintiffs.

foreseeable.[133] As it is a form of SLADA, no finding of fault or defect is necessary for liability to take hold.

Once a platform has grown such that it becomes inherently dangerous, it will need to "experiment with methods of preventing accidents that involve . . . relocating, changing, or reducing (perhaps to the vanishing point) the activity."[134] While eliminating the activity altogether is not productive, for dangerous internet platforms, this could mean a cap on the reach of accounts of some public figures.[135] Platforms could be forced to implement expensive measures like human verification of posts or requiring even more substantial security procedures on certain high-profile accounts.[136] One commentator suggests that strict liability and "cyber insurance" should be tightly coupled as a means to implement strict liability for data breaches while simultaneously statutorily limiting damages, ensuring the willingness of insurance companies to underwrite policies.[137] Such a scheme would also help to mitigate a possible economic concern that could result from implementation of SLADA across the industry, specifically, the cascading, shifting of costs to consumers as a result of the specter of no-fault findings of liability.[138]

Finally, the unmistakable social value that dangerous internet platforms provide does not conflict with the application of SLADA:

---

[133] Baker v. Saint-Gobain Performance Plastics Corp., 232 F. Supp. 3d 233, 248 (N.D.N.Y. 2017) ("[A] private suit for damages [might lie] when an individual or smaller group sustains a special loss that is different in kind from the harm suffered by the rest of the community.") (internal quotation omitted). The challenging burden of identifying market segments particularly vulnerable to compromise should fall to the platform providers.

[134] *Ind. Harbor Belt*, 916 F.2d at 1177 (citation omitted).

[135] *See* Joshua Boyd, *The Most Followed Accounts on Twitter*, BRANDWATCH (Oct. 1, 2020), https://www.brandwatch.com/blog/most-twitter-followers/ [https://perma.cc/7LHW-T6CH] (cataloging Twitter accounts with tens or hundreds of millions of followers).

[136] *See About Account Security*, TWITTER, https://help.twitter.com/en/safety-and-security/account-security-tips [https://perma.cc/QKG7-RGXF] (last visited Oct. 2, 2020). For example, two-factor authentication or updated client recommendations could be mandated.

[137] *See* Hurwitz, *supra* note 28, at 1499–1500.

[138] *See id.* at 1527–29.

> [SLADA] rests on the assumption that the activity's advantages are apparently substantial enough as to render reasonable the defendant's choice to engage in the activity . . . . [T]he point that the activity provides substantial value or utility is of little direct relevance to the question whether the activity should properly bear strict liability . . . . [I]t is their commonness rather than their value that directly pertains to the strict-liability issue.[139]

SLADA's suggested application here is not meant to deter platforms from existing or even prospering, but rather to exercise extreme caution when its casual use by public figures ushers in catastrophic risk.

B. Abnormally Dangerous Activities and the Goals of SLADA

The reorganized Restatement (Third) of Torts moved SLADA into a volume subtitled "Physical & Emotional Harm," calling into question its applicability to purely economic loss.[140] However, the revised strict liability section is prefaced by stating that "strict liability is one area of tort law in which a page of history can be at least as relevant as a page of logic."[141] Therefore, this section surveys the policy goals underlying the doctrine and adds to the growing mass of commentary arguing that strict liability should be considered by courts in the context of insecure software.[142]

One American Law Institute reporter distilled the revised Third Restatement's scattered rationales for SLADA into six elements which will be briefly considered in turn against the proposed application.[143] First, the additional liability imposed by SLADA is meant to encourage defendants engaging in dangerous activities to

---

[139] RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 20 cmt. k (AM. L. INST. 2010).

[140] *Id.* at foreword.

[141] *Id.* at ch. 4 scope note.

[142] Scott, *supra* note 7, at 469 n.267; *see also* Citron, *supra* note 95, at 277–96. *But see* Choi, *supra* note 89, at 51–52 (arguing that SLADA is an outdated form of strict liability and that strict products liability or no-fault insurance are better doctrinal fits).

[143] *See* Kenneth W. Simons, *The Restatement (Third) of Torts & Traditional Strict Liability: Robust Rationales, Slender Doctrines*, 44 WAKE FOREST L. REV. 1355, 1359 (2009).

take even more care than they would under a negligence regime.[144] This rationale is predicated on the theory that the marginal cost of reducing risk beyond a negligence standard of care is small.[145] Additionally, many abnormally dangerous activities are so destructive that it is often impossible for plaintiffs to obtain the evidence needed for a showing of breach.[146] Strict liability incentivizes defendants in those situations to take more enhanced precautions than they would take in an ordinary negligence regime.[147]

This rationale militates both for and against SLADA for dangerous internet platforms. The costs of incremental improvements to security for internet platform providers are certainly not just marginal, and indeed may increase without bound.[148] The fact that substantially better security is not necessarily achievable even with substantial additional investment distinguishes this risk from the ones contemplated by the Restatement. On the other hand, establishing evidence of causation in a negligence suit might well be difficult or impossible.[149]

Second, SLADA is meant to apply a corrective to the magnitude or frequency of dangerous activities.[150] Limiting "activity" is antithetical to the modus operandi of internet platforms that depend on the network effect for increased

---

[144] *Id.* at 1359 (citing the example of explosives destroying proof that would be needed for a finding of negligence).

[145] RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 21 cmt. d (AM. L. INST. 2010) ("[Because] in most instances a reasonable nonnegligent fence will succeed in restraining the defendant's livestock, the added burden that strict liability places on the livestock owner is itself limited.").

[146] *See* Klein v. Pyrodyne Corp., 810 P.2d 917, 922 (Wash. 1991) (imposing strict liability when a fireworks misfire destroyed all evidence of what caused the misfire).

[147] *See* Simons, *supra* note 143, at 1359.

[148] *See* Rainer Böhme, *Security Metrics and Security Investment Models*, 5 INT'L WORKSHOP ON SEC. 10, 11 fig.1 (2010).

[149] *See* Scott, *supra* note 7, at 448–49; *supra* Section III.D.

[150] *See* Simons, *supra* note 143, at 1360.

revenues.[151] However, if the dangerous "activity" is instead defined as that portion of the platforms' operations involving exposure to abnormal danger, as opposed to routine use, it can be reduced in creative ways by internet platforms.[152] If exposed to liability under a SLADA theory, platforms might be forced to implement expensive measures like human verification of publications or to require even more substantial, onerous security procedures on certain high-profile accounts, perhaps to the point of discouraging use.[153]

Third, SLADA is justified when the defendant's activity imposes a risk on individual members of society that does not reciprocally impose risk back on the defendant.[154] Users of dangerous internet platforms are exposed to a variety of risks, and their perceptions of those risks to themselves and third parties vary widely according to their level of sophistication.[155] The platform providers, on the other hand, are surely fully cognizant of the risks of compromise, and are themselves potentially exposed to those risks.

Along the same lines, the fourth rationale concerns non-reciprocal benefit: whether the dangerous activity confers a benefit on the defendant not shared by the members of the community.[156] A converse statement of the "common usage" prong of the SLADA Restatement criteria, this rationale highlights that "the appeal of strict liability for an activity is stronger when its risks are imposed on third parties while its benefits are concentrated among a few."[157] However, while the benefits of

---

[151] *See* Feng Zhu & Marco Iansiti, *Why Some Platforms Thrive and Others Don't*, HARV. BUS. REV., https://hbr.org/2019/01/why-some-platforms-thrive-and-others-don't [https://perma.cc/35V8-D7LS] (last visited Oct. 2, 2020).

[152] *See infra* Section V.A.

[153] *See* Boyd, *supra* note 135 and accompanying text.

[154] Simons, *supra* note 143, at 1361–62.

[155] *See, e.g.,* Paul van Schaik et. al, *Security and Privacy in Online Social Networking: Risk Perceptions and Precautionary Behaviour*, 78 COMPUT. IN HUM. BEHAV. 283, 292–93 (2018) (presenting an analysis of perceptions of risk and precautionary behavior among Facebook users).

[156] Simons, *supra* note 143, at 1363–66.

[157] RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 20 cmt. j (AM. L. INST. 2010).

using an internet platform can fairly be described as diffuse, the benefits received by high-profile actors, like heads of state, are of a different kind entirely from those obtained by, say, teenagers. For example, the ability to globally announce a major policy change is not, in practice, shared by most users, who are enjoying the platforms for social reasons.[158] The benefits to the platform providers, on the other hand, scale roughly with numbers of users, whatever benefit those users may derive from it, and affected third parties might receive no benefit at all. In other words, the bulk of the benefits are retained by the platform providers and a small number of elite users.

Fifth, application of SLADA is associated with near-exclusive causation, a characterization fraught with philosophical hangnails.[159] Regardless of the difficulties of pinning down the definition of causation in the context of dangerous internet platforms, if the scope of liability is limited to non-users, the case for exclusive causation is even stronger than the canonical example of blasting, wherein the injured resident could (theoretically) simply move.[160] SLADA is "designed largely to protect innocent third parties or innocent bystanders."[161] The potential pecuniary harm caused by dangerous internet platforms will exist as long as large numbers of individuals rely on it, which is something an individual plaintiff cannot control.

Sixth, the Restatement affords weight to the community's sense of fairness: "Basic public attitudes tend to be accepting of familiar and traditional risks, even while apprehensive of risks that are uncommon and novel. The law should be respectful of public

---

[158] *See* Aaron Smith, *Why Americans Use Social Media*, PEW RSCH. CTR. (Nov. 15, 2011), https://www.pewresearch.org/internet/2011/11/15/why-americans-use-social-media/ [https://perma.cc/APS3-LQT3] ("Roughly two thirds of social media users say that staying in touch with current friends and family members is a major reason they use these sites.").

[159] *See* Simons, *supra* note 143, at 1368–72 ("[I]t is either incoherent or false to claim that the person who engages in blasting is the only or principal cause of the victim's harm.").

[160] RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 20 cmt. k (AM. L. INST. 2010).

[161] *Id.* § 24.

attitudes of this sort."[162] It is hard to say how the public at large would perceive the fairness of strict liability for dangerous internet platforms under these circumstances; the phenomenon of damages at this scale is too new to predict. But it might be equally said that the public does not appreciate the danger posed by these apparently innocuous tools. It might also be labeled unfair that an accident due to the lax security practices of a moderately-sized private company in California can have instantaneous, severe, or nationwide repercussions at all.

The goals of SLADA as delineated by the Third Restatement are consonant with the risks dangerous internet platforms force on society. But application of the doctrine will nevertheless face substantial obstacles erected by common law precedent.

C. Obstacles in Applying SLADA to Dangerous Internet Platforms

An application of SLADA to non-physical, purely economic damages to third parties due to the malicious actions of cybercriminals encounters substantial precedential hurdles. Here, the first subsection circumvents the traditional application of SLADA only to physical harms with recourse to underlying policy goals. The next subsection recasts the ordinary common usage objection in light of the way modern technology is actually used. Then, a route around the bar against damages for purely economic harms is identified. Finally, the last subsection argues that that route should be exploited to avail plaintiffs of tort liability to redress damages caused by the actions of third-party criminals where a special relationship due to foreseeability exists.

1. Physical Damages

At early common law, injuries in tort were generally associated with direct contact, and fault was seen as related to the physical actions of the defendant.[163] SLADA evolved during the industrial revolution as a parallel path to liability alongside negligence, usually portrayed as growing out of the decision in *Rylands*.

---

[162] Simons, *supra* note 143, at 1372–73 (quoting RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 20 cmt. j (AM. L. INST. 2010)).

[163] *See* King, Jr., *supra* note 112, at 343–44.

"*Rylands* is the first and foremost exemplar of the strict liability alternative to negligence liability for accidental personal injury and property damage."[164] As the doctrine homogenized across the country, neither the First nor the Second Restatements specified "physical" harm in their respective SLADA sections, specifying only serious harm to the person, land or chattels of others.[165] The Third Restatement explicitly added "physical harm," but the comments and reporters' notes do not explicitly rule out non-physical damages.[166]

Despite these recent updates, some courts still relying on the Second Restatement have shown flexibility regarding non-physical damages.[167] For example, in *Peters v. Amoco Oil Co*.,[168] when underground leaking storage tanks belonging to an oil company bled into neighboring properties, but had not yet caused any physical damage, a district court in Alabama rejected the defendant's motion to dismiss the SLADA claim, interpreting the Restatement to "not require physical contact or damage, and [finding that the] Defendants [failed] to provide any authority containing such requirement."[169]

In another groundwater contamination suit against oil companies, *Harthman v. Texaco, Inc.*,[170] a district court rejected the defendant's summary judgment motion, interpreting the Restatement's requirement for "harm" in SLADA cases broadly as "[including] the impairment of pecuniary advantage, intangible rights and other legally recognized interests" and holding that the

---

[164] Abraham, *supra* note 99, at 226.

[165] RESTATEMENT (FIRST) OF TORTS §§ 519–20 (AM. L. INST. 1938); RESTATEMENT (SECOND) OF TORTS § 520 (AM. L. INST. 1977).

[166] RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 20 (AM. L. INST. 2020). However, the definition of "physical harm" provided does militate strongly against this interpretation. *See id.* at § 4.

[167] *See, e.g.,* Brantley v. Int'l Paper Co., No. CV 2:09-230-DCR, 2017 WL 2292767, at *5 (M.D. Ala. May 24, 2017) ("[E]xpansion of the doctrine to other activities has not been foreclosed.").

[168] Peters v. Amoco Oil Co., 57 F. Supp. 2d 1268 (M.D. Ala. 1999).

[169] *Id.* at 1286.

[170] Harthman v. Texaco, Inc. (In re Tutu Wells Contamination Litig.), 909 F. Supp. 991 (D.V.I. 1995).

plaintiff "may recover for negligence or strict liability without showing that they have suffered physical harm."[171]

Beyond interpretations of what the reporters of the Restatement intended, convincing a court to apply SLADA to non-physical damages requires recourse to the policy justifications of SLADA, which are not themselves necessarily linked to physical harms.[172] Advocates should focus on the novel nature and foreseeability of abnormal danger in lieu of the black-letter Restatement text.

2. Common Usage

The "common usage" prong of the Restatement's SLADA test ensures that the doctrine is only enforced against "abnormal" activities.[173] An activity is one of common usage if "it is carried on by a large fraction of the people in the community."[174] This is so even if the activity is engaged in by only a single party, even if substantial numbers of people are somehow "connected to the activity."[175] When considering SLADA for new technologies like "cyber-physical" systems, one scholar warns that "technological novelty should not be conflated with abnormality."[176]

Still, while it is undeniable that dangerous internet platforms are in extremely common usage, the metaphors used to exemplify common usage do not graft well onto this case. At first glance,

---

[171] *Id.* at 999 (invoking the Restatement (Second) of Torts general definition of "harm" in section 7, cmt. b and broadly interpreting the wording of section 519, "harm to the person, land or chattels"); RESTATEMENT (SECOND) OF TORTS § 7 cmt. b (AM. L. INST. 1977); RESTATEMENT (SECOND) OF TORTS § 519(1) (AM. L. INST. 1977); *see also* Exxon Corp. v. Yarema, 516 A.2d 990, 1006 (Md. Ct. Spec. App. 1986) ("Case law in other jurisdictions also supports the proposition that plaintiffs may recover for economic injuries that defendant's pollution caused, even though there was no physical damage to plaintiffs' property.").

[172] *See supra* Section V.B.

[173] RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 20 cmt. j (AM. L. INST. 2020).

[174] *Id.*

[175] *Id.*

[176] Choi, *supra* note 89, at 51 (considering looming examples such as autonomous vehicles deployed in dense residential areas as unlikely to be found to be abnormally dangerous).

dangerous internet platforms could be analogized to power lines.[177] Like power lines, access to the platforms is distributed to the community via the internet, itself physically a network of wires.[178] The power company is said to be "engaging in the [abnormally dangerous] activity," but since the distribution network—the wires—are ubiquitous, people are "connected to the activity" and power lines are therefore in common usage.[179]

However, this analogy oversimplifies the presence of power lines in society. Residences receive standard residential power connections, with well-understood safety considerations. On the other hand, industrial installations have extremely high-power demands, involving more significant safety procedures, unattainable by normal power consumers.[180] Dangerous internet platforms place the industrial connection in the palms of prominent public figures who similarly lack the ability to implement improved security. Additionally, unlike power lines, which are a physical embodiment of a danger in common usage, there is no physical reminder, or indeed any reminder at all during routine use, that internet platforms could pose any sort of catastrophic danger.[181] Finally, while social media posts taken as a whole are nothing short of torrential, the discrete uses of dangerous internet platforms by actors capable of effecting severe consequences on markets constitute only a minute fraction of total uses.[182]

---

[177] RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 20 cmt. j (AM. L. INST. 2010).

[178] *Id.*

[179] *Id.*

[180] *See, e.g.,* Dennis K. Neitzel, *Electrical Safety for Industrial and Commercial Power Systems*, 2016 IEEE IAS ELEC. SAFETY WORKSHOP, 114, 115–20 (summarizing safety procedures for industrial and commercial power systems).

[181] *Twitter Terms of Service*, TWITTER, https://twitter.com/en/tos [https://perma.cc/6K9M-MC98] (last updated June 18, 2020) (waiving liability for "ANY CONDUCT OR CONTENT OF ANY THIRD PARTY ON THE SERVICES, INCLUDING WITHOUT LIMITATION, ANY DEFAMATORY, OFFENSIVE OR ILLEGAL CONDUCT OF OTHER USERS OR THIRD PARTIES").

[182] *Compare Twitter Usage Statistics*, INTERNET LIVE STATS, https://www.internetlivestats.com/twitter-statistics/ [https://perma.cc/KZ5W-FWTE] (last visited Oct. 18, 2020) (counting hundreds of millions of Tweets sent globally each day), *with National Politics on Twitter: Small Share of U.S. Adults*

Another example of a commonly used and omnipresent utility with underappreciated inherent destructive power involves the underground gasoline storage tanks underlying typical gas stations.[183] Although the activities of a gas station in providing gas, and the reciprocal activities of a patron in purchasing and pumping gas are obviously quite familiar, the threat posed by a catastrophic failure of these tanks while standing atop them is potentially uncommon, although courts are split on this question.[184] No bright-line rule has been identified. For example, in *Peters*, a federal court found the question of whether the storage of gasoline would constitute an "unusual and extraordinary" use of property to be a fact-bound question for the jury.[185]

Still, American courts have shown an overall reluctance to push the boundaries of common usage since the emergence of another potentially spectacularly powerful source of risk in the middle of the twentieth century: nuclear energy.[186] Moreover, what is considered common usage varies widely between jurisdictions, implying a reluctance by courts to make bright-line rules about strict liability and reinforcing the context-dependent nature of the common usage determination.[187] Also, humanity's relationship to risk has become more comfortable as people have become surrounded by technology, and life, at least relative to technology, has in fact become safer.[188] Nevertheless, these observations about context and technology in the history of the common law mean only that where the doctrine has once moved in one direction, it can move again where technology has changed in ways never anticipated.[189]

Produce Majority of Tweets, PEW RSCH. CTR. (Oct. 23, 2019), https://www.pewresearch.org/politics/2019/10/23/national-politics-on-twitter-small-share-of-u-s-adults-produce-majority-of-tweets/ [https://perma.cc/TA7B-H5W6].

[183] RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 20 reporter's notes to cmt. j (AM. L. INST. 2010).

[184] *Id.*

[185] Peters v. Amoco Oil Co., 57 F. Supp. 2d 1268, 1286 (M.D. Ala. 1999).

[186] Abraham, *supra* note 99, at 224.

[187] *Id.*

[188] *Id.*

[189] *Id.* at 227 ("We study *Rylands* not only because of what it was and is, but also because of what it might have been and might still become.").

3. Purely Economic Loss

Another formidable obstacle faced by a plaintiff affected by a compromise of an internet platform causing significant, lasting pecuniary fallout is the economic loss rule.[190] Commonly stated as there can never be recovery for purely economic loss in a tort action,[191] the Third Restatement more fully states that "there is no liability in tort for economic loss caused by negligence in the performance or negotiation of a contract between the parties."[192]

The economic loss doctrine is largely predicated on the notion that the risk of purely economic loss should be allocated exclusively according to contract law.[193] The doctrine assumes that the consequential damages flowing from the accident are the result of the plaintiff's disappointed expectations.[194] In other words, the economic loss doctrine assumes the existence of a contract in the first place.[195]

As between strangers with no contractual relationship, the majority of jurisdictions follow the *532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Center, Inc.*[196] decision.[197] In *532 Madison Ave. Gourmet*, the New York Court of Appeals held that monetary damages to neighboring businesses stemming from the economic fallout due to a collapsed, negligently constructed building were foreclosed, absent some special relationship between the parties.[198] The court focused on the unlimited spectrum of liability that defendants might be exposed to under these circumstances, stating: "however careless the conduct or foreseeable the harm . . . [t]his

---

[190] Scott, *supra* note 7, at 470–71.

[191] Rustad & Koenig, *supra* note 8, at 1580.

[192] RESTATEMENT (THIRD) OF TORTS: LIAB. FOR ECON. HARM § 3 (AM. L. INST. 2020).

[193] Jeffrey L. Goodman, Daniel R. Peacock & Kevin J. Rutan, *A Guide to Understanding the Economic Loss Doctrine*, 67 DRAKE L. REV. 1, 17–26 (2019) (describing the majority rule: "if the plaintiff suffers purely economic damages, the plaintiff's only avenue of recovery is through contract").

[194] *Id.*

[195] Johnson, *supra* note 63, at 547–48.

[196] 532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Ctr., Inc., 750 N.E.2d 1097 (N.Y. 2001).

[197] Catherine M. Sharkey, *Can Data Breach Claims Survive the Econ. Loss Rule?*, 66 DEPAUL L. REV. 339, 348–49 (2017).

[198] *532 Madison Ave. Gourmet Foods, Inc.*, 750 N.E.2d at 1101–03.

restriction is necessary to avoid exposing defendants to unlimited liability to an indeterminate class of persons conceivably injured by any negligence in a defendant's act."[199] But in no-contract scenarios, the rationale for the economic loss rule that emphasizes the primacy of the separate domains of contract and tort law is not applicable.[200] Moreover, a minority of jurisdictions have shown a willingness to depart from the orthodoxy of the economic loss rule, particularly when a foreseeable, identifiable class of plaintiffs is available in lieu of unlimited liability.[201]

Some courts have considered and rejected the invocation of SLADA for purely economic loss.[202] For example, in *Rosenblatt v. Exxon Co.*,[203] a tenant tried to sue the former owner of a tract of land whose actions resulted in toxic contamination of the land by gasoline for the economic losses resulting from failed business opportunities. The court found the relationship between the tenant and former landowner to be too attenuated.[204]

Thus, these holdings and the requirement for a bounded set of plaintiffs suggest that a more substantial relationship between prospective plaintiffs and the platform provider defendant must be identified to recover economic losses, which courts have found through foreseeability.[205] High-profile users of dangerous internet platforms will each map to different foreseeable sets of plaintiffs; anticipating the scope of a potential compromise might be a daunting task for platform providers, but seems a reasonable

---

[199] *Id.* at 1101.

[200] 532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Ctr., Inc., 271 A.D.2d 49, 52 (N.Y. App. Div. 2000) (citing Robins Dry Dock & Repair Co. v. Flint, 275 U.S. 303 (1927)) ("[A] claimant suffering purely financial losses is restricted to an action in contract for the benefit of its bargain.").

[201] Sharkey, *supra* note 197, at 358–60.

[202] *See e.g.,* In re One Meridian Plaza Fire Litig., 820 F. Supp. 1460, 1476–1477 (E.D. Pa. 1993) ("[P]laintiffs cannot circumvent the economic loss doctrine by its allegations of strict liability based on an abnormally dangerous activity.").

[203] Rosenblatt v. Exxon Co., U.S.A., 642 A.2d 180 (Md. 1994).

[204] *Id.* at 188.

[205] *See infra* Section V.C.4.

burden to fall on the shoulders of the enterprise that stands to benefit most from the celebrity voice of its users.[206]

Another route around the precedential wall erected by the economic loss doctrine, as suggested by Professor Citron in 2007, imagines reconceptualizing the nature of torts for the Information Age.[207] In contrast to a self-worth defined by the ability to perform physical work with their bodies and property, Citron posits that "individuals [now] define themselves by their interactions and integrity in the marketplace" and that therefore "the law should adapt to account for injuries to our changed conception of personhood in the twenty-first century."[208] Such a reconceptualization would include economic damages related to, for example, the fallout from a data breach.[209]

Since 2007, however, dangers posed by the internet have grown enough that a reconceptualization of the nature of potential tort damages is no longer necessary. Citron compares the metaphor relating reservoirs of data to *Rylands*' reservoirs of water, but the metaphorical parallels between the two types of "reservoirs" are less important than the actual fact of extreme danger.[210] The common law should include these extreme dangers among those considered abnormally dangerous.

4. Tort Liability for Third-Party Criminals

Without a statutory basis for liability, the starting point for building a case for any sort of common law liability consists in showing that the internet platform providers can be held liable for the actions of third-party criminals. The canonical case on-point is *Kline v. 1500 Massachusetts Ave. Apartment Corp.*,[211] where a duty to protect as between landlords and tenants was identified when the landlord had actual or constructive notice of a threat to the

---

[206] *See, e.g.*, Meiring de Villiers, *Reasonable Foreseeability in Info. Sec. Law: A Forensic Analysis*, 30 HASTINGS COMM. & ENT. L.J. 419, 471–75 (2008) (developing a metric for estimating the foreseeability of compromise in cybersecurity contexts).

[207] Citron, *supra* note 95, at 295–96.

[208] *Id.*

[209] *Id.* at 296.

[210] *Id.* at 279.

[211] Kline v. 1500 Mass. Ave. Apartment Corp., 439 F.2d 477 (D.C. Cir. 1970).

tenants.[212] Scholars have argued that this holding should be applied to the relationship between computer database operators and subjects of data breaches, whose identities could be compromised in the event of a breach.[213]

Thus, a finding of liability against a compromised dangerous internet platform depends on the identification of a duty between the parties, a legal theory that exists only in nascent form in the realm of software security.[214] However, since *Kline*, the DC Circuit has further refined the relationship required between parties and indicated that a legal duty might not always be required: "If the relationship . . . strongly suggests a duty of protection, then specific evidence of foreseeability is less important, whereas if the relationship is not of a type that entails a duty of protection, then the evidentiary hurdle is higher."[215] In other words, even without a legal duty, if the damage was highly foreseeable, a defendant can still be found liable for the actions of third parties.[216]

Outside of the DC Circuit, some courts have eliminated the duty requirement in light of substantial foreseeability in the context of data security. In *In re Arby's Restaurant Group Inc. Litigation*,[217] a federal court applied Georgia law and found a common law duty where hackers stole the credit card data of

---

[212] *See generally id.* at 481 ("The rationale of the general rule exonerating a third party from any duty to protect another from a criminal attack has no applicability to the landlord-tenant relationship . . . [The landlord] certainly is no bystander. [Where he] has notice . . . and has the exclusive power to take preventive action, it does not seem unfair to place upon the landlord a duty to take those steps which are within his power to minimize the predictable risk to his tenants.").

[213] Johnson, *supra* note 63, at 572–76; Citron, *supra* note 95, at 261–63 n. 116; Rebecca Crootof, *The Internet of Torts: Expanding Civil Liability Standards to Address Corporate Remote Interference*, 69 DUKE L.J. 583, 630–33 (2019) (considering the identification of a duty between "Internet of Things" companies and their users).

[214] Rustad & Koenig, *supra* note 8, at 1586–76; Johnson, *supra* note 63, at 575–76; *see supra* Section III.D.

[215] Workman v. United Methodist Comm., 320 F.3d 259, 264 (D.C. Cir. 2003).

[216] Ridgell v. HP Enter. Servs., LLC, 209 F. Supp. 3d 1, 21 (D.C. 2016) (quoting Potts v. D.C., 697 A.2d 1249, 1252 (D.C. 1997)).

[217] In re Arby's Rest. Grp. Inc. Litig., No. 1:17-CV-0514-AT, 2018 WL 2128441 (N.D. Ga. Mar. 5, 2018).

hundreds of thousands of consumers, holding that "allegations that a company knew of a foreseeable risk to its data security systems are sufficient to establish the existence of a plausible legal duty."[218] As argued *supra*, compromises of dangerous internet platforms are not only foreseeable, they are inevitable.[219]

VI. CONCLUSION

There is a large chasm to cross before a court will agree to apply the doctrine of SLADA to dangerous internet platforms. Common law precedent holding the rule to apply only in the context of a narrowly defined subset of property damages, along with the longstanding economic loss rule, will require a court to make a bold step away from longstanding legal doctrines. But SLADA "is tort law's conscience, an always-available alternative to the negligence system that persistently causes us to examine the justifications for the limitations on liability that are inherent in [existing tort law]."[220]

The threat posed by certain internet platforms with global reach, used daily by governments and world leaders, was obviously not anticipated by the aggregated authors of those precedents. It is becoming progressively less controversial to argue that these internet platform providers should be exposed to liability in some form for consequences stemming from preventable compromises of their software security, especially given the

---

[218] *Id.* at *5; *see also* In re: The Home Depot, Inc., Customer Data Sec. Breach Litig., No. 1:14-MD-2583-TWT, 2016 WL 2897520, at *4 (N.D. Ga. May 18, 2016) ("A retailer's actions and inactions, such as disabling security features and ignoring warning signs of a data breach, are sufficient to show that the retailer caused foreseeable harm to a plaintiff and therefore owed a duty in tort."); In re Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1320 (N.D. Ga. 2019) (comparing "criminal data breaches to the peculiarly similar context of premises liability where [at least one court] has held that if a proprietor has reason to anticipate a criminal act, then he or she has a duty to exercise ordinary care to guard against injury from dangerous characters.") (internal quotations omitted).

[219] *See supra* Section II.C.

[220] Abraham, *supra* note 99, at 207. Abraham believes that the impact of *Rylands* and SLADA theory generally is minimal and out of proportion with its actual adoption in US jurisdictions since the mid-twentieth century.

unjustifiable immunity usually found to exist under Section 230 of the Communications Decency Act.[221] It is for jurists to decide what form that will take, unless and until Congress takes action. In the case of the most extreme dangers posed by these platforms, the analog to the dangers originally observed by the *Rylands* court are clear: such platforms must either assume liability for the consequences of compromises that are certain to occur, or else they must cease to exist in their current abnormally dangerous form.

It took some twenty years after *Rylands* was decided in England before American courts adopted the doctrine.[222] Even greater than the gradual forces of change associated with industrialization and economic growth, some commentators draw a direct line between particular massive disasters and the adoption of SLADA in the United States, notably the Johnstown Flood of 1889 in Pennsylvania, in which the South Fork Dam in the outskirts of Pittsburgh burst and killed over 2,000 due to the negligence of wealthy country club owners.[223] Perhaps we must wait until a cyber-Johnstown occurs; or perhaps it has already happened.

---

[221] *See generally* Citron & Wittes, *supra* note 68 (proposing a judicial overhaul of Section 230 jurisprudence based on reasonable precautions).

[222] Citron, *supra* note 95, at 275; *see also* Jed H. Shugerman, *The Floodgates of Strict Liability: Bursting Reservoirs and the Adoption of Fletcher v. Rylands in the Gilded Age*, 110 YALE L.J. 333, 334–35 (2000).

[223] Citron, *supra* note 95, at 275; Peter Smith, *Johnstown Flood of 1889: Greatest Disaster in the State Continues to Resonate*, PITTSBURGH POST-GAZETTE (May 24, 2014, 11:57 PM), https://www.post-gazette.com/news/state/2014/05/25/Johnstown-Flood-of-1889-continues-to-resonate/stories/201405250142 [https://perma.cc/3F59-YZRN] ("A jury of Pennsylvania Lutherans, Reformed Dutch, Presbyterians, Methodists, Baptists or Catholics will not take readily to the attempt to cast the responsibility of such a catastrophe from the shoulders of the fine rich gentlemen who owned the fish pond and the rotten dam to the shoulders of God.") (quoting *The Law of Bursting Reservoirs*, 23 AM. L. REV. 643, 647 (1889)).