2017

Cyberensuring Security

Justin Hurwitz

CONNECTICUT
LAW REVIEW

VOLUME 49 SEPTEMBER 2017 NUMBER 5

Article

Cyberensuring Security

JUSTIN (GUS) HURWITZ

Cybersecurity is one of the most pressing and legally difficult issues facing this country today. It touches every aspect of modern political and social life, the economy, and national security. From the OPM and IRS breaches, to the Sony hack, to attacks on hospitals and health insurers, to attacks on domestic and international infrastructure, to domestic and international surveillance, cybersecurity concerns are omnipresent. For technical, legal, and practical, reasons, they also have proven extremely difficult to address.

This Article draws from the economic literatures on strict liability and insurance to argue that cyber incidents generally, and data breaches specifically, should be treated as strict liability offenses. But that is only the starting point of this Article's argument. The economic literature on strict liability recognizes that it is, in fact, a form of insurance—potential tortfeasors subject to strict liability effectively are required to insure others against harms caused by their conduct. This Article's core argument is that pervasive cyber-incident insurance is the best approach to addressing the full range of cybersecurity concerns.

The characteristics of the model proposed in this Article compare favorably to the current status quo—one in which users are largely helpless, firms are largely unknowledgeable, software is generally insecure, federal agencies are generally impotent to bring about meaningful change, and attackers are largely judgement-proof. As an initial matter, it would offer consumers redress when cyber-incidents occur. But more importantly, it would facilitate education about and monitoring of cybersecurity practices; it would facilitate the collection, analysis, and use, of aggregate information about the causes and costs of these incidents; and it would put that information the hands of parties in a position to improve the existing ecosystem.

ARTICLE CONTENTS

Cyberensuring Security

JUSTIN (GUS) HURWITZ [*]

INTRODUCTION

Cybersecurity is one of the most pressing and legally difficult issues facing the Internet today. It touches every aspect of modern political and social life, the economy, and national security. From the breaches of the Office of Policy & Management (OPM) and the Internal Revenue Service (IRS), to the Sony hack, to attacks on hospitals and health insurers, to attacks on domestic and international infrastructure, to domestic and international surveillance, cybersecurity concerns are omnipresent. For reasons technical, legal, and practical, cybersecurity concerns have proven extremely difficult to address.

In recent years researchers have debated several possible mechanisms for improving the overall state of the cybersecurity ecosystem. Two of the most frequently advanced ideas are bringing cybersecurity-related harms

[*] Assistant Professor of Law, University of Nebraska College of Law. J.D., University of Chicago, 2007; M.A. (economics), George Mason University, 2010; B.A., St. John's College, 2003. With particular thanks to Sasha Romanosky, David Opderbeck, David Thaw, Jay Kesan, participants at the 2017 *Connecticut Law Review* Annual Symposium, the 2016 GMU Law & Economics Center Digital Information Policy Scholars Conference, and the 2016 *South Carolina Law Review* Annual Symposium. Additional thanks to the staff of the *Connecticut Law Review* for their excellent work bringing this Article to print, and to Will Nelson and Kevin Adler for research assistance on this and other projects. This is a complex and rapidly developing area, so this Article is necessarily incomplete and unquestionably contains errors—all such infirmities are attributable to myself or APT 29. It is my hope that, despite these infirmities, this Article advances the discussion about the relationship between cyber insurance and cybersecurity.

under a strict-liability regime[1] and use of cyber insurance.[2] Both ideas have

[1] *See*, *e.g.*, Stephen E. Blythe, *Contractual Liability of Suppliers of Defective Software: A Comparison of the Law of the United Kingdom and United States*, 26 NW. J. INT'L L. & BUS. 77, 93–94 (2005) (recommending that U.S. contract laws may need to be reformed to "provide additional protection for the buyer who hurriedly purchases software online without bothering to read an often lengthy agreement containing legalese"); 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 (2007); Michael Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?,* 67 MD. L. REV. 425, 469–70 (2008) (explaining arguments for and against applying strict tort liability to defective software, and noting that "[o]ver the last twenty years, there have been calls to impose strict product liability on software vendors for defects"); Frances E. Zollers et al., *No More Soft Landings for Software: Liability for Defects in an Industry That Has Come of Age*, 21 SANTA CLARA COMPUTER & HIGH. TECH. L. J. 745, 768–73 (2005) (arguing that strict liability should be imposed on software manufacturers to serve public policy); *see also* Jon Evans, *Should Software Companies Be Legally Liable for Security Breaches?*, TECHCRUNCH (Aug. 6, 2015), https://techcrunch.com/2015/08/06/should-software-companies-be-legally-liable-for-security-breaches/ (discussing the inevitability of software liability); Dennis Fisher, *Software Liability is Inevitable*, THREATPOST (Aug. 5, 2015, 2:19 PM), https://threatpost.com/software-liability-is-inevitable/114136/ ("The push for some form of liability for vendors who sell faulty or insecure software is nearly as old as software itself. . . . the day may soon come when software liability is a reality."); Jake Kouns & Joshua Corman, *Software Liability? The Worst Possible Idea (Except for All Others)*, RSA CONFERENCE 2014, https://www.rsaconference.com/writable/presentations/file_upload/asec-f01-software-liability-the_worst-possible-idea-except-for-all-others_final.pdf (last visited Feb. 23, 2017) (presenting arguments and counterarguments for software liability); Bruce Schneier, *RSA 2012: Are Software Liability Laws Needed?*, SCHNEIER ON SEC. (Mar. 1, 2012), https://www.schneier.com/news/archives/2012/03/rsa_2012_are_softwar.html ("[L]iability laws [will] transfer the economic cost for faulty software from the user to the developer and provide an incentive for the developer to fix the problem."). *See generally* David Berke, *Products Liability in the Sharing Economy*, 33 YALE J. ON REG. 603, 640–48 (2016) (describing the beneficial effects that strict liability for software would have on the sharing economy); James A. Henderson, *Tort vs. Technology: Accommodating Disruptive Innovation*, 47 ARIZ. ST. L.J. 1145, 1159–60, 1168–70 (2015) (observing that though disruptive technological innovations are protected by a lack of strict product liability, products liability law already has procedural safeguards to protect the developers of disruptive innovations).

[2] *See, e.g.*, *Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities: Hearing Before the H. Comm. on Armed Services*, 115th Cong. 8 (2017) (statement of P.W. Singer, strategist at New America) (available at http://docs.house.gov/meetings/AS/AS00/20170301/105607/HHRG-115-AS00-Wstate-SingerP-20170301.pdf []); Gregory D. Podolak, *Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today's Litigation, and Tomorrow's Challenges*, 33 QUINNIPIAC L. REV. 369, 398 (2015) (discussing the rise of cyber insurance); Jay P. Kesan & Carol Mullins Hayes, Strengthening Cybersecurity with Cyber Insurance Markets and Better Risk Assessment (Feb. 27, 2017) (Univ. of Illinois College of Law Legal Studies Research Paper No. 17-18) (available at https://ssrn.com/abstract=2924854 []) Jay P. Kesan et al., *Cyberinsurance as a Market-Based Solution to the Problem of Cybersecurity—A Case Study* 34–35 (Jun. 2, 2005) (paper delivered at Fourth Workshop on the Economics of Information Security [hereinafter WEIS]) (available at http://infosecon.net/workshop/pdf/42.pdf []) (arguing that the cyber insurance industry is evolving and can inform best practices once a few remaining challenges are worked out); Jay P. Kesan et al., *The Economic Case for Cyberinsurace* 30–31 (Univ. of Ill. College of Law, Law and Econ. Working Papers, Paper No. 2, 2004) (available at http://law.bepress.com/cgi/viewcontent.cgi?article=1001&context=uiuclwps []); Marc Lelarge & Jean Bolot, *Economic Incentives to Increase Security in the Internet: The Case for Insurance* 8–9 (Apr. 19, 2009) (paper delivered at 2009 International Conference on Computer Communications [hereinafter IEEE Infocom.]) (available at http://www.di.ens.fr/~lelarge/papiers/2009/infocom09_cr.pdf []) (finding that cyber insurance could

substantial merit—but they also face substantial obstacles. Perhaps the greatest criticism of each is the impracticality of implementation, as both face serious practical and logistical problems. For instance, merely implementing a strict liability rule doesn't address a key problem with current liability regimes: determining damages for cybersecurity-related harms. Moreover, mandating that firms purchase insurance policies does not address many insurers' reluctance to underwrite broad coverage; while the cyber insurance market has grown dramatically in recent years, it is still small and policies are written narrowly.

This Article's key contribution to the issue is the observation that strict liability and cyber-insurance are complementary sides of a single coin. A strict-liability regime could make it dramatically easier to overcome the key challenges facing widespread adoption of cyber insurance policies and a more vibrant insurance marketplace could help overcome the key challenges that are preventing the adoption of strict-liability rules for cyber incidents. This observation offers helpful insights into ongoing discussions about both strict liability and cyber insurance—insights that are useful to both subject areas independently, as well as important as a way to bring these discussions under a common framework.

This Article draws from the economic literatures on strict liability and insurance to understand their relationship in the cybersecurity context. The economic literature on strict liability recognizes that it is, in fact, a form of insurance. Potential tortfeasors subject to strict liability are effectively required to insure others against harms caused by their conduct.[3] Drawing from that insight, this Article proposes a strict-liability rule for harms deriving from cyber-incidents. Under this rule, consumer-facing firms that use or store consumer information would be strictly liable to those consumers for any security incidents (i.e., data breaches) involving that data. In order to work, this rule would impose administratively defined statutory

---

incentivize entities to invest in self-prevention and thereby increase the security of the internet); Parinaz Naghizadeh & Mingyan Liu, *Voluntary Participation in Cyber-Insurance Markets* 3–5 (Jun. 23, 2014) (paper delivered at WEIS 2014) (available at http://www.econinfosec.org/archive/weis2014/papers/NaghizadehLiu-WEIS2014.pdf []) (proposing a cyber insurance mechanism); Ranjan Pal et al., *Will Cyber-Insurance Improve Network Security? A Market Analysis* 9 (Apr. 27, 2014) (paper delivered at IEEE Infocom. 2014) (available at http://www-bcf.usc.edu/~kpsounis/Papers/cyberinsurance_infocom2014.pdf []) (discussing how the potential of cyber insurance to improve network security is hampered by a need for profitable insurance mechanisms).

[3] *See infra* Part V.A. (discussing the interplay between strict liability and cyber insurance); *see also* Richard A. Epstein, *Products Liability as an Insurance Market*, 14 J. LEG. STUDS. 645, 654 (1985) (discussing how an implicit expectation that liability insurance will be available is built into the rules of products liability); George L. Priest, *The Current Insurance Crisis and Modern Tort Law*, 96 YALE L.J. 1521, 1586 (1986) (stating that the initial judicial expansion of third-party liability was motivated by a desire to protect the poor, and discussing the first adoption of strict liability); Steven Shavell, *On Liability and Insurance*, 13 BELL J. OF ECON. 120, 121 (1982) (discussing insurance risk allocation under strict liability).

damages, but firms that have cyber insurance policies covering third-party harms would only pay the lesser of those statutory damages or actual provable damages for insured claims.

The characteristics of this model compare favorably to the current status quo—one wherein users are largely helpless, firms are largely unknowledgeable, software is generally insecure, federal agencies are generally impotent to bring about meaningful change in the structure and operation of private markets, and attackers are largely judgement-proof. As an initial matter, it would offer consumers redress when cyber-incidents occur. But, more importantly, insurance and insurers play a regulatory role. They collect and study information about best practices, they train and educate their customers, they engage with other institutional actors in ways that can improve the overall quality of the security ecosystem, and they lobby for legislative and regulatory changes that reduce their exposure to risk—which, in the security context, means lobbying to reduce overall risk.[4]

This Article proceeds in five sections. Sections I and II provide an introduction to the reasons that cybersecurity is challenging. Section I focuses on why it is hard to secure systems, including technical, institutional, and economic reasons. Section II builds on this discussion by considering why it has proven difficult for the law to regulate and improve cybersecurity practices.

Sections III and IV discuss strict liability and cyberinsurace as potential ways to overcome the limitations discussed in Section II—approaches that may improve the overall cybersecurity ecosystem. Both ideas have enough merit that they have been advanced many times over the years as potential solutions to cybersecurity challenges. But both also face substantial hurdles that have limited their viability.

Section V synthesizes the discussion in Sections III and IV. This synthesis begins with the assertion that strict liability is, from an economic perspective, a form of insurance. Counterintuitively, strict liability does not encourage firms or individuals to take greater care to avoid harming parties to whom they are strictly liable. Rather, the incentive is to invest the same amount in avoiding harms as one would under an ordinary negligence rule. Should a harm nonetheless occur, the strictly liable party bears the burden of compensating the harmed party—that is, it insures the harmed party against that risk. This suggests—and this Article argues—that imposing strict liability on firms hosting consumer data would achieve the key purposes of cyber insurance that have so far remained elusive, and it would do so in a way that addresses some of the key challenges generally facing the use of strict liability to address cybersecurity issues.

---

[4] *See infra* Section IV.B (discussing the regulatory role and functions of insurance and insurers in the security ecosystem).

I. THE CHALLENGE

Computer security, especially for Internet-connected devices, presents hard problems. This Section offers a brief overview of the technical, practical, and some legal difficulties of protecting data in the online environment.

The discussion offered below—both in this Section and throughout this Article—frames "cybersecurity" primarily in terms of data security and data breaches. It is important for any reader new to cybersecurity to understand that these are only two subsets of the cybersecurity field, even though many of the highest-profile cybersecurity incidents involve data breaches. And for those more familiar with the field, it is important to define the scope of this Article's discussion as focusing on the data-breach context. The policy framework developed in Section V, in particular, focuses on the data-breach context—or, more precisely, on the relationship between consumers and consumer-facing firms that store consumer data. At the same time, the benefits of this proposal would almost certainly redound to the broader cybersecurity ecosystem.

A. *The Ex Ante Cybersecurity Challenge*

The basic task of cybersecurity would seem simple: to ensure that those, and only those, authorized to access data or computers systems are allowed to do so.[5] The difficulties of accomplishing this easily stated task, however, are myriad. We can begin with just scoping the elements of the task: we need a way to specify who does and does not have access to a secured system, a way to identify those users, and a way to specify and control the level of access they may have. This problem quickly decomposes into requirements to specify and authenticate individual users, specify the various resources they may be able to access, and specify various levels of access each user is granted to each resource.[6] The number of combinations of users, resources, and permitted access levels permutes quickly, imposing substantial costs (mostly in the form of managing a complex system) both on those managing and those using the secured system.

Indeed, this complexity is one of the fundamental tradeoffs in the world of security: allow for finer-grained control—which increases complexity, imposes higher burdens on those subject to the security model, and increases

---

[5] Critically, the task of "security" is fundamentally different from that of "privacy." Security is about prohibiting *unauthorized* parties from accessing or using data or systems; privacy is about prohibiting *authorized* parties from exceeding the use of data to which they have been given access. *See* Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667, 669 (2013) (discussing the distinctions between privacy and security).

[6] *See, e.g.*, Carl Landwehr, *Formal Models for Computer Security*, 13 ACM COMPUTING SURVEYS 247, 250 (1981) (discussing the greatly heightened security complexities of electronic versus paper documents).

the likelihood that mistakes in implementing that model will be made, leading to security faults—or reduce the complexity of the system—which requires either allowing some users greater access to secured resources than is necessary or denying some trustworthy users access to resources of which they would otherwise be able to make beneficial uses.[7] By analogy, imagine designing an office building with a lock on every door, each requiring a unique key, and providing employees with individual keys to each room to which they are allowed access. Obviously, no office would actually operate in this way, because the burdens on both the office management and individual employees would be prohibitive. This analogy also demonstrates another of the fundamental tradeoffs in designing secure systems: if the cost of complying with security protocols is too great, users may find ways to bypass those protocols.[8] This too is most easily seen by example: in the physical world, one may prop doors open instead of continually unlocking them; in the world of computers, users may leave passwords written on post-it notes, or use the same password for all of their online activity.[9]

The challenge created by complexity is much more problematic in the case of computer security than in the physical world. This is because every aspect of computer security needs to be implemented in computer code. There are two basic reasons why this is difficult. First, it requires every aspect of the security protocols to be *completely* specified *ex ante*, and,

---

[7] *See, e.g.*, Alexander DeWitt & Jasna Kuljis, *Is Usable Security an Oxymoron?*, 13 ACM INTERACTIONS 41, 43 (2006) (indicating that increased sophistication of cybersecurity programs leads to increased opportunities for user error).

[8] *See* STEVEN M. BELLOVIN, THINKING SECURITY: STOPPING NEXT YEAR'S HACKERS 248–49 (2016) (discussing the tendency of employees and systems users to ignore or workaround intrusive security measures).

[9] One of the basic truths of security is that users are one of, if not the primary, security vulnerabilities. Substantial attention has been focused on studying user behavior and the relationship between system design and user behavior. Despite these efforts, designing systems that encourage security aligned user behavior continues to be a central challenge. *See generally*, Anne Adams & Martina Angela Sasse, *Users Are Not the Enemy*, 42 COMMS. OF THE ACM 40 (1999); Elissa M. Redmiles et al, *How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior*, PROCEEDINGS OF THE 2016 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 666 (2016); Ryan West, *The Psychology of Security: Why Do Good Users Make Bad Decisions?*, 51 COMMS. OF THE ACM 34 (2008); Kenneth Olmstead & Aaron Smith, *What the Public Knows About Cybersecurity*, PEW RES. CTR. (Mar. 22, 2017), http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/ []; Marc van Zadelhoff, *The Biggest Cybersecurity Threats Are Inside Your Company*, HARV. BUS. REV. (Sept. 19, 2016), https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company []; Cormac Herley, *So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users* (Sept. 2009) (paper delivered at the 2009 New Security Paradigms Workshop); Ruogu Kang et al, *"My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security* (July 2015) (paper delivered at SOUPS 2015 Symposium on Usable Privacy and Security) (available at https://www.usenix.org/system/files/conference/soups2015/soups15-paper-kang.pdf []); Alma Whitten & J.D. Tygar, *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0* (Aug. 1999) (paper delivered at the 8th USENIX Security Symposium) (available at https://www.usenix.org/legacy/events/sec99/full_papers/whitten/whitten_html/index.html []).

second, these security protocols must be specified (in computer code) *accurately*. Again taking the physical world as a counter-example: one need not "program" a door to allow the fire department access in the event of an emergency (either humans will intervene and, smelling smoke, allow entrance, or the door will be forcibly opened); one need not "program" employees to comply with a court order or warrant; and individual actors can accommodate many otherwise incompletely specified actions on an ad-hoc basis. For example, an employee could make photocopies for a contractor who does not have a copier code.[10] In the computer context, each of these actions would need to be specified *ex ante*—otherwise the system may need to be taken offline and reprogrammed, or circumvented on a case-by-case (and likely complex) basis. Of course, one can imagine implementing computer-based security protocols in a way that allows for greater human discretion (e.g., a bank teller could review every online-transaction a user makes, or a system administrator could confirm a user's credentials each time she logs into a system). But doing so would defeat one of the basic purposes of computer-based interactions: removing humans from routinized transactions so that those transactions can proceed at computer-scale, not human-scale, speeds.

The problem of *accurate* implementation is even more substantial than that of complete implementation. Indeed, one of the foundational theorems in computer science—the so-called "halting problem"—states that it is effectively impossible to prove that any computer code beyond a trivial level of complexity operates as intended (that is, that it contains no bugs, such as those that could render a security protocol ineffective).[11] We need not delve into the mathematical proofs that show the near impossibility of proving that a given piece of computer code is defect-free. Rather, we can point to some of the canonical examples of basic implementations mistakes in security-related software.[12] Examples include the Heartbleed bug,[13] bugs in the

---

[10] Or, to take a canonical example from the literature, see Andrew Odlyzko, *Cryptographic Abundance and Pervasive Computing*, U. OF MINN. DIGITAL TECHNOLOGY CTR., http://www.dtc.umn.edu/~odlyzko/doc/crypto.abundance.txt (last visited Mar. 1, 2017) ("A key problem with strong information security in an office environment is that it would stop secretaries from forging their bosses' signatures. A good assistant exercises judgement and handles routine matters without increasing the load on the boss.").

[11] Mark C. Chu-Carroll, *Basics: The Halting Problem*, SCI. BLOG (Feb. 6, 2007), http://scienceblogs.com/goodmath/2007/02/06/basics-the-halting-problem/ [].

[12] *See* Ross Anderson, *Why Cryptosystems Fail*, 1 ACM CONF. ON COMPUTER & COMM. SECURITY 215, 218–21 (1993) (detailing common implementations mistakes and corresponding security vulnerabilities in ATM operating systems); Bruce Schneier, *Security Pitfalls in Cryptography*, 6 INFO. MGMT. & COMPUTER SECURITY 133, 134–35 (1998) (discussing basic implementations mistakes and the security vulnerabilities they expose).

[13] *See The Heartbleed Bug*, CODENOMICON, http://heartbleed.com (last visited Mar. 1, 2017) (describing the Heartbleed Bug, "a serious vulnerability in the popular OpenSSL cryptographic software library").

Apache TLS implementation,[14] attacks on encryption Certificate Authorities,[15] the Shellshock bug,[16] and critical encryption flaws in Apple iMessage[17] and LastPass.[18] Each of these is an example of code developed and scrutinized, often for years, by sophisticated, security-conscious programmers that nonetheless contained critical flaws in how they were implemented.[19] In other words, at a technical level security is hard—very hard—to do correctly.

B. The ex post Cybersecurity Challenge

The issues discussed above relate to the challenges of designing and implementing a system that is secure—that is, a system that prevents unauthorized activity. But this is only one part of the cybersecurity challenge. Because no system is completely secure, any sound security design needs to anticipate and respond to security breaches. Incident response presents its own slate of problems, including technical challenges similar to those that make designing and implementing secure systems difficult, physical-world problems relating to coordinating human resources to respond to incidents, and legal challenges.

The gold-standard for approaching security is the NIST Cybersecurity

---

[14] *See* David Adrian et al., *Weak Diffie-Hellman and the Logjam Attack*, WEAKDH, http://weakdh.org (last visited Mar. 1, 2017) (describing a flaw in the TLS Internet protocol that can be exploited by a Logjam attack, allowing the attacker to read and modify data being passed over a secure connection).

[15] *See* BLACK TULIP: REPORT OF THE INVESTIGATION INTO THE DIGINOTAR CERTIFICATE AUTHORITY BREACH, FOX-IT 59 (2012), https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf (reporting on a MITM attack on the Diginotar Certificate Authority, whereby the intruder was able to issue rogue certificates granting access to virtually any common software).

[16] *See* Symantec Security Response, *Shellshock: All You Need to Know about the Bash Bug Vulnerability*, SYMANTEC OFFICIAL BLOG (Sept. 25, 2014), https://www.symantec.com/connect/blogs/shellshock-all-you-need-know-about-bash-bug-vulnerability (advising on a vulnerability in Bash, a widely used Linux command language interpreter).

[17] *See* Ellen Nakashima, *Johns Hopkins Researchers Poke a Hole in Apple's Encryption*, WASH. POST (Mar. 21, 2007), https://www.washingtonpost.com/world/national-security/johns-hopkins-researchers-discovered-encryption-flaw-in-apples-imessage/2016/03/20/a323f9a0-eca7-11e5-a6f3-21ccdbc5f74e_story.html?utm_term=.d7e1e6cb42fe [https://perma.cc/EP5E-EB2Z] (reporting on a vulnerability in Apple iMessage that allowed attackers to retrieve a photo from Apple's servers).

[18] *See* Joe Siegrist, *LastPass Security Notice*, LASTPASS (July 10, 2015, 8:00 PM), https://blog.lastpass.com/2015/06/lastpass-security-notice.html/ (discussing a recent security breach).

[19] As another class of examples, consider cases in which elite security professionals themselves suffer security incidents. *See, e.g.*, Swati Khandelwal, *Phone-Hacking Cellebrite Got Hacked; 900GB of Data* Stolen, HACKER NEWS (Jan. 12, 2017), http://thehackernews.com/2017/01/mobile-hacking-cellebrite.html (stating that a company that sells hacking tools was hacked); J.M. Porup, *How Hacking Team Got* Hacked, ARSTECHNICA (Apr. 19, 2016, 9:36 AM), https://arstechnica.com/security/2016/04/how-hacking-team-got-hacked-phineas-phisher/ (detailing how an experienced hacker suffered a hack on his own system).

Framework.[20] At the most general level, this framework defines five core security functions that must be part of an organization's cybersecurity activity. These functions start with *identifying* the "systems, assets, data, and capabilities" that need to be secured. Systems then need to be developed to *protect* these resources. Recognizing that no system is ever entirely secure, the next function of the framework is to put in place systems to *detect* the occurrence of cybersecurity events. When such an event is detected, the next step is to *respond* to it: for instance, by activating pre-established incident response plans, containing the scope of the event's impacts, and taking steps to mitigate its impacts. Finally, once the incident is contained and its causes corrected, an organization's final function is to *recover* from the incident by restoring backups, reinitializing systems, and the like. Critically, the framework is process-oriented. Each of these steps is an ongoing process, subject to ongoing improvement and refinement on its own and as lessons are learned from each of the other steps.

Detection is likely the hardest of these functions to implement. Systems need to be designed to allow for the detection of security breaches. Here, as above, the task of programming computers for this task is far more difficult than analogous physical-world challenges. To start, secured systems need to have monitoring capabilities that can observe and record how they are used. This is an onerous, and at times intractable, task. Adding such capabilities can substantially reduce system performance, such that any monitoring instrument needs to be deployed sparsely. We also face the same challenge of implementing it correctly. Attackers therefore already have two attack vectors: attack resources that are either unmonitored or ineffectively monitored. What is more, it is frequently the case that an attacker who breaches a secured system simultaneously (or as a result of the breach) obtains access to the system's monitoring capabilities. Generally, avoiding this conundrum requires implementing additional separate monitoring and logging systems (that is, computers)—but this has the unfortunate consequence of increasing overall system complexity even further, which can actually make it easier for breaches to occur.

One function of well-implemented monitoring tools is to detect security incidents in real time. But monitoring also serves the important function of recording system activity for later use and analysis. The simplest aspect of this is allowing for the reconstruction of incidents. Reconstruction serves at least three important purposes: to figure out how an attack occurred so that future attacks can be prevented, to understand the effects of the attack (e.g., to see what data was compromised), and to serve as evidence for identifying and taking action against those responsible for the attack.

---

[20] The discussion below is modeled around the structure developed in the NIST Cybersecurity Framework. *See* NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 7 (2014) (stating the core elements of the framework as: identify, protect, detect, respond, and recover).

But there is another equally important purpose behind monitoring: establishing a baseline of normal system operation. Unfortunately, data is rarely analyzed for these purposes. This is one of the reasons that the second part of the monitoring equation is rarely satisfactorily met: the ultimate purpose of *monitoring* a system is to *detect* abnormal behavior.

The seemingly key function of detecting attacks is often the most challenging to accomplish. In most computer security breaches investigated by security consulting firms, the attackers breach a system several months before their breach is detected. In this time, they may be engaged in malicious activity (such as exfiltrating information, or manipulating internal information to harm an attack target), or they may be using their initial breach as a beachhead to further penetrate the target's systems.

Once a breach has been detected, incident response becomes the order of the day. The first step in incident response is to mitigate any ongoing effects of the breach. For instance, compromised systems should be disconnected from any networks, sensitive accounts should be locked down, and appropriate resources should be engaged (e.g., law enforcement or security professionals). Here too, proper response can be both technical and difficult. For instance, one of the most important things to *not* do upon discovering a compromised system is to turn the system off—even though this is the intuitive response. Turning the system off will delete potentially important information stored in the computer's memory and terminate any active programs which could be used to figure out the source and scope of the attack. In addition, turning a system back on can overwrite similarly important information.

Once the effects of the incident have been mitigated, the compromised party can turn to responding to the attack. This may include any number of efforts. For instance, a compromised system should be repaired, and the source or cause of the compromise fixed to prevent future incidents. Parties harmed by an attack should generally be notified, both as a matter of best practices and often as a function of relevant law. Compromised data or systems may need to be replaced or repaired. The victims of an attack may want to work with law enforcement, insurers, or vendors to identify or take action against the attackers. The victims of an attack may also want or need to take legal action of their own (e.g., to bring a civil suit against their attackers, if possible, or to defend themselves against suits brought by the government or as a class action). Discussion of the viability, practicalities, and limitations of such legal action are the subject of Section II.

C. *The Multiplicity of Actors*

The technical difficulties of designing secure computer systems are dramatically compounded by the sheer number of actors in the security ecosystem. It is useful to identify these actors here, before discussing how

their (often conflicting) incentives further complicate computer security.[21]

On one far side of the web, we have "users"—those who actually use a (possibly) secure system. Even this basic unit of the ecosystem is more complicated than one would expect. Users can refer to the consumer end-users of a piece of software, such as Microsoft Windows. In a firm, users may refer to the employees of the firm who use software purchased or designed by the firm. The firm itself may be said to be the user of software purchased for use by its employees, or even of software that it designed (or bespoke software designed by a contractor). And, of course, the firm's customers are users of services offered by the firm, which may or may not rely upon systems designed or implemented by third parties.

Those third parties may be firms such as Microsoft, Apple, Google, or ExamSoft. They could also be vendors that sell turnkey solutions, designed by themselves or by others. They may be contractors, who design bespoke systems. Or they may be "integrators," who integrate various platforms designed by third parties with a firm's own systems. Connecting all of these systems are various Internet-based entities. These include the ISPs that connect firms to the Internet, or a firm's customers to the firm's servers and services. It also includes cloud-based services, which often host information.

All of these relationships quickly explode into a complex network of relationships and dependencies—or, in more legalistic terms, reliance interests, duties, and potential liabilities. Consider a firm storing its customers' information on a cloud-storage service that it integrated into its back-end systems (running Microsoft Windows) using proprietary software written by a contractor that relies on the application program interface (API) provided by both Microsoft and the cloud provider. If the proprietary software leaks the customers' confidential information due to a previously unknown problem with how Microsoft's API interacts with the cloud provider's API, who is liable?

Now let's add into this mix cyber-physical systems and Internet of Things devices: your modern, Internet-connected car, with literally hundreds of networks and computers running a range of software—including location-aware software that automatically turns your home's heating system to energy-saving mode when you leave the house and unlocks your front door when you return. Some of the software running on your car's computers is commercial software, some of it was developed internally by the car manufacturer's own software development team, and some of it is "open-

---

[21] In addition to the discussion presented below, *see, e.g.*, Johannes M. Bauer & Michael J.G. van Eeten, *Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options*, 33 TELECOM POL'Y 706, 708 (2009) ("Information and communication services require inputs from many players. They include internet service providers (ISPs), application and service providers (App/Svc), hardware and software vendors, users, security providers, and national and international organizations involved in the governance of these activities."); Susan Tisdale, *Cybersecurity: Challenges From a Systems, Complexity, Knowledge Management and Business Intelligence Perspective,* 16 ISSUES INFO. SYSTEMS 191, 192–93 (2015) (detailing the need for cooperation and exchange between stakeholders).

source software" that has been developed over the years by an army of hundreds or thousands of anonymous volunteers whose commitment to the quality of the software only runs as deep as their possibly transient interest in working on open-source projects as a way to learn the basics of computer programming.

This multiplicity of actors makes establishing cybersecurity responsibility difficult. Each of the actors has some legitimate argument that at least some of the others bear responsibility for almost any cyber-incident. Software was poorly designed or integrated, systems were improperly implemented or managed by firms or their contractors, ISPs should have detected harmful activity by malicious actors and informed their targets or cut off access, firms failed to train or monitor their employees, employees failed to comply with established procedure, customers chose to work with unknown firms that had unknown or poor security practices, or firms failed to have satisfactory security practices. The response to any security incident will invariably be to assign blame to any number of other parties.

It is notable that responsibility for security breaches is rarely meaningfully attributed to the parties that are actually responsible: the attackers behind the cyber-incident.[22] This is a nod to the practical reality that it is often impossible to identify the attackers, that it would typically be almost impossible to bring suit against the attackers if it were possible to identify them, and that even then, a victim would be unlikely to recover meaningful damages from them. Amazingly enough (and as discussed in Section II), even if the victim could find the attacker, given the challenges discussed throughout this Section, it would be very difficult to establish the elements required to be awarded damages against him. Given the multiplicity of actors and difficulties of designing secure systems, it can be difficult, if not impossible, to establish causation and (especially) harm. As a result, it often makes more sense to seek legal recourse against one of the many intermediary actors, even when they were not in a meaningful position to prevent a given harm. This is the canonical case of the data breach, where damages (when they are sought) are almost always sought against the firm that experienced the data breach and are almost never sought against the actual parties that caused the breach (either as attackers or for having designed or implemented insecure systems).

On a final note, it is useful to discuss briefly the multiplicity of harms that may result from a cyber-incident—or, stated alternatively, the

---

[22] On the topic of attribution, see JEFFREY HUNKER ET AL., INST. FOR INFO. INFRASTRUCTURE PROT., ROLE AND CHALLENGES FOR SUFFICIENT CYBER-ATTACK ATTRIBUTION 5 (2008) (defining attribution and the difficulties associated with it); Jon R. Lindsay, *Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack*, 1 J. CYBERSECURITY 53, 54 (2015) (stating that attribution is particularly difficult because attackers depend on deception to obfuscate their identities).

multiplicity of motivations that attackers may have.[23] Starting with the most apparent motivations that attackers may have: they may seek to obtain information through hacking. This could be information about a firm's customers (e.g., passwords, personal information, correspondence, credit-card information), or about the firm itself (as in the case of espionage). They may also intend to damage a firm, for instance by altering or deleting sensitive information or damaging physical systems controlled by compromised computers. Attackers may use "ransomware" to demand money from a target. The compromised systems may in fact not even be an intended target: they could be a platform that attackers use in attacking other third-party systems. Or attackers may have political or social purposes: they may intend to embarrass a firm or individuals, to cause reputational damage, or to advance a political agenda.

This range of motivations further demonstrates the challenges discussed thus far. For instance, if one expects attackers to target sensitive customer information, it may be possible to address this risk by minimizing the amount of customer information that is stored and encrypting what information must be kept. It is more difficult, however, to prevent control systems from being used to damage the systems that they control—to do so would undermine the purpose of having computerized control systems. This also demonstrates what will be an important challenge discussed in detail below: establishing harm for the purposes of liability. How should a court measure the harm caused by an attack that shuts down a firm for a few hours, or results in the disclosure of (truthful) information about a firm's customers, or that is the basis forcing the firm to adopt a new policy as part of a political agenda? Courts are generally reluctant to award damages for harms such as these—they are simply too speculative and difficult to measure.

D. *The Multiplicity of (Conflicting) Incentives*

Each of the myriad actors in the cybersecurity ecosystem faces their own incentives in deciding how or whether to respond to security concerns.[24] While each would likely benefit from an improved cybersecurity ecosystem, none has strong incentives to invest substantially in such benefits. And

---

[23] *See* David Thaw, *Criminalizing Hacking, Not Dating*, 103 J. CRIM. L. & CRIMINOLOGY 907, 916 (2013) (stating that hackers hack for financial gains); *see also* Robin Gandhi et al., *Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political*, 30 IEEE TECH & SOC'Y MAG. 28, 29 (2011) ("It is also now known that cyber-attackers' level of socio-technological sophistication, their backgrounds, and their motivations, are essential components to predicting, preventing, and tracing cyber-attacks.").

[24] *See* Ross Anderson & Tyler Moore, *Information Security: Where Computer Science, Economics and Psychology Meet*, 367 PHIL. TRANSACTIONS OF ROYAL SOC'Y 2717, (2009) (discussing the various factors to consider when deciding whether to respond to security concerns, such as economic considerations).

many, in fact, have incentives to adopt bad security practices.

One of the most basic—and pernicious—causes of problematic incentives in cybersecurity is externalities.[25] Externalities exist where the private costs or benefits that accrue to one party as a result of a given act do not incorporate the costs or benefits that befall third parties. The gap between first- and third-party effects is called an externality.[26] The canonical example is that of air pollution: it has often been the case that factories were free to use the air as a free resource, polluting it without regard to how that pollution affected third parties. Because the owner of the factory does not bear the harmful effects of air pollution she will over-use the air, creating negative third-party effects that would not occur if these costs were borne by the factory owner.[27] Unfortunately, given the multiplicity of actors in the cybersecurity ecosystem, cybersecurity is characterized by pervasive externalities.[28]

Another important set of incentives echoes the fundamental tradeoffs between security and usability described in Section I.A. Both users and those designing software and other computer systems are generally willing to forego security for greater usability and performance. This results in large part from the difficulty of holding designers liable for defective software—the threat of legal liability would of course be a powerful incentive for firms to improve their products' security. This is further exacerbated by firms' ability to attribute fault for security incidents to others in the security ecosystem—including attributing fault to users themselves. This reduces firms' ability (or need) to compete along a security dimension—especially when consumers are often more responsive to the usability and short-term cost dimensions. And there is reason to argue that users do, in fact, bear some responsibility for the poor state of the cybersecurity ecosystem: despite professed fears about the collection and use of sensitive data and widespread concern about cybersecurity, consumers very readily engage in conduct online that exposes them to risks.[29] This is surely, in some part, a reflection of putatively irrational decision making by consumers. It is also, to some extent, a form of rational ignorance: consumers are not security experts, nor do they have the time or knowledge necessary to evaluate most firms'

---

[25] *See* Anderson & Moore, *supra* note 24; *see also* Bauer & van Eeten, *supra* note 21, at 710 ("Many of the challenges of reaching an optimal level of information security at the aggregate level are rooted in a potential mismatch between the perceived individual and social benefits and costs of security."); Nathan Alexander Sales, *Regulating Cyber-Security*, 107 N.W. U. L. REV. 1503 (2013).

[26] Sales, *supra* note 25, at 1519–20.

[27] For further discussion of this concept, see Sales, *supra* note 25; Bauer & van Eeten, *supra* note 21, for concise discussions.

[28] Bauer & van Eeten, *supra* note 21, at 707 (explaining that, while private actors face many incentives to improve security, "significant externalities remain that cannot easily be overcome by private action").

[29] *See, e.g.*, Kenneth Olmstead, *Americans and Cybersecurity*, PEW RES. CTR. (Jan. 26, 2017), http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/ ("[M]any Americans are failing to follow digital security best practices in their own personal lives . . . .").

security practices, and they reasonably believe that the law will protect them should they be harmed by malfeasant firms. Thus, it is reasonable for consumers to engage in what appears to ordinary users to be ordinary online activities.

Similarly, firms that make use of third-party security systems in their broader business—that is, the vast majority of firms—face poor security incentives. Most security incidents target firms' customers' information, such that the firms themselves are unlikely to experience any loss from an attack—that is unless news of the attack becomes public, in which case a firm may face substantial reputational harms and may also bear some direct costs from responding to the attack. In other words, the incentive for most firms is to invest in very basic security—only enough to secure their systems from casual attackers—and otherwise pay no attention to security. These incentives were arguably even worse before the recent, and relatively widespread, adoption of state data-breach notification laws[30]—laws that require firms to notify affected consumers of data breaches that may affect their (the consumers') data. Before the adoption of such laws, firms often faced no incentive to disclose or even to respond to a data breach, and were incentivized to keep the fact of the breach secret. But even following adoption of these laws, firms still do not face substantial incentives to adopt strong security practices. This is in part because there is still little likelihood that a firm will be held liable for damages resulting from a data breach. More tragically, this is also largely because consumers have become inured to data breaches, such that the reputational harm to a firm of a data breach is much less today than it was even two or three years ago.

Perhaps the worst incentives are faced by the cybersecurity industry itself. Estimates vary, but the size of the cybersecurity "market"—comprising firms that specialize in various aspects of cybersecurity, from systems design, to consulting, incident response, and litigation—is currently pegged at somewhere around $75-100 billion.[31] This amount is expected to grow to $170 billion by 2020,[32] a growth rate significantly exceeding that of other parts of the economy. In other words, the status quo is working well and industry participants have little reason to improve the state of the cybersecurity ecosystem.[33]

---

[30] *See* NAT'L CONF. ST. LEGISLATURES, SECURITY BREACH NOTIFICATION LAWS (Feb. 24, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (providing an overview of the state laws).

[31] Steve Morgan, *Worldwide Cybersecurity Market Continues Its Upward Trend*, CSO (July 9, 2015, 5:47 AM), http://www.csoonline.com/article/2946017/security-leadership/worldwide-cybersecurity-market-sizing-and-projections.html [].

[32] *Id.*

[33] For one colorful discussion of this reality, see Iain Thompson, *GCHQ Cyber-Chief Slams Security Outfits Peddling "Medieval Witchcraft,"* REGISTER (Feb. 3, 2017, 7:03 AM), https://www.theregister.co.uk/2017/02/03/security_threat_solutions/ (stating that the cybersecurity community is opposed to spreading unfounded fear and uncertainty in an effort to sell products).

II. PROBLEMATIC SOLUTIONS

Section I discussed why cybersecurity is difficult as a technical and practical matter. This Section looks at the difficulties of using the law to address cybersecurity concerns. It starts by considering the relationship between legal and technical institutions. It then considers the challenges that private law institutions have faced in responding to cybersecurity incidents, followed by consideration of the efficacy to date of public law institutions.

A. Law and Technology as Complementary Approaches to Cybersecurity

As discussed in Section I, there are many reasons why cybersecurity is a legitimately difficult problem. It is technologically difficult to specify what is required of a secure system, it is extremely difficult to accurately implement the system once specified, and it is effectively impossible to verify that such a system is implemented correctly. Moreover, the costs of security in terms of design, implementation, performance, and user experience are substantial enough that they are often not justified by their benefits. This is particularly problematic when we consider the private incentives faced by almost every actor in the security ecosystem: almost no actor has strong incentives that are in line with best security practices, and almost every actor has strong incentives that run contrary to best security practices.

None of these problems, however, are new. Many systems and institutions are difficult to design or implement properly. Indeed, it is a basic fact of life that mistakes and accidents happen, and that people are often harmed by those mistakes. Moreover, it is often the case that individuals' private incentives do not align with socially optimal conduct. Cybersecurity presents extreme cases of all of these problems.

Society manages to continue moving along despite these challenges largely because the law operates as a backstop that mitigates the harms that may result from them. The law steps in when things go wrong. In general, it does so through two mechanisms. First, it compensates parties that are harmed by bad actors or bad actions. In other words, it assures users of a system that if they are acting reasonably and are harmed by another actor who is acting unreasonably, they can be compensated for that harm. Second, it makes clear that parties who cause harm to occur are liable for that harm. This in turn creates incentives for those who create systems used by others to do so carefully—to design their systems so that they will not cause undue harm—because they will be responsible for compensating others for those harms.

Law and technology are complementary approaches to the design of

well-designed systems.[34] We want systems to be well designed ex ante so as to limit harms. The availability of ex post remedies ensures that those designing systems will be held to account for their design decisions. At the same time, the law recognizes that risk is inevitable and mistakes may happen. So the law generally works to assign liability for harms in ways that maximize the social value of activity, mitigating concerns that individual actors will be motivated solely by their private incentives at the expense of imposing costs on society.

But this synergy between law and technology assumes the presence of effectively designed and implemented legal rules. As suggested in Section I, the legal rules relating to cybersecurity have proven wholly ineffective. This has had the unfortunate consequence of exacerbating cybersecurity problems—as described in Section I, many actors in the cybersecurity ecosystem not only lack incentives to act well, but have incentives to act badly. These incentive mismatches result largely from the lack of effective legal rules.

The rest of this Section discusses the failings of current legal approaches to addressing cybersecurity concerns. This will provide a foundation for the discussion in Sections III and IV, presenting an alternative approach to these concerns.

B. *Private Law Approaches to Cybersecurity*

"Private law" refers broadly to legal causes of action that individuals are able to bring against one another. For instance, suits for trespass, breach of contract, or negligence are traditional private law causes of action. So too would be a civil cause of action created by statute that can be initiated by individuals, or a class action brought by a group of individuals. This is in contrast to "public law" causes of action, which are generally those initiated by the government. These include, for instance, criminal prosecutions, enforcement actions brought by regulatory agencies, rules created by federal agencies with which regulated parties must comply, and various forms of informal regulation exercised by government actors to channel the conduct of private parties.

Private law institutions have proven largely ineffective at addressing cybersecurity concerns for much the same reason that cybersecurity is itself difficult. In order to successfully bring a civil lawsuit, one needs to be able to demonstrate various things, such as the identity of the actors that caused

---

[34] The canonical contemporary discussion of this is offered by Lawrence Lessig. *See* Lawrence Lessig, *The New Chicago School*, 27 J. LEG. STUDS. 661, 672 (1998) ("The aim of the New Chicago School is to speak comprehensively about these tools—about how they function together, about how they interact, and about how law might affect their influence. These alternative constraints beyond law do not exist independent of the law; they are in part the product of the law."); *see also* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

a harm; that they, in fact, did cause that harm; that the harm is legally cognizable; and that there is some adequate measure of damages. Each of these elements is difficult in the context of cybersecurity. The multiplicity of actors in the security ecosystem and the complexity of the interactions between them makes it difficult, and sometimes impossible, to attribute fault to any specific actor.[35] And even when fault can be attributed to a single actor, there are likely other confounding factors (or actors) that make it difficult to prove that the actor's conduct was a proximate cause of the specific harm.[36] For instance, a firm that failed to safeguard its customers' information may argue that the software it was using was defective, that the vendor hired to install and maintain its software failed to do so correctly, that an auditing firm it hired to ensure its systems were properly secured failed to detect the relevant faults, that its network providers failed to detect or alert it to suspicious activity, or even that the customers were contributorily negligent in providing their data to an untrustworthy party.

Even if the harmed party can demonstrate that a specific actor's conduct was improper and proximately caused an adverse security incident, courts have struggled with the concept of "harm" online—both in terms of recognizing that the subject of the cyber-incident has in fact experienced harm and in assessing the extent of that harm for purposes of damages.[37] The canonical example here is the disclosure or theft of personal information. In one canonical case, for instance, courts found that an airline's disclosure of passenger information to the federal government's antiterrorism efforts was

---

[35] *See* David W. Opderbeck, *Cybersecurity, Data Braches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935, 938 (2016) ("When everything is connected, a breach at one node of the network potentially affects all nodes, or a multiplicity of nodes, in unpredictable, non-linear ways. Can tort law play any principled role in managing this risk?").

[36] This is most often seen in the context of the economic loss doctrine. *See id*. at 968–69 ("There is no 'stream' of causality, but rather a non-linear 'web' of causes and effects, running backward and forward, up and down, in and out, under and around. In one sense, this should make the duty/proximate cause/economic loss analysis easier: outside the immediate 'proximity' of the breach, determining the probability of loss with any reasonable certainty might prove impossible. In another sense, however, the difficulty of showing which affected parties are 'upstream' and which are 'downstream' of something like the Michigan Avenue Bridge could mean that tort law cannot perform its traditional functions of deterring excessively risky conduct, encouraging risk mitigation strategies, and adjusting the social costs of externalities.").

[37] For a discussion of the extent of damages resulting from a security incident, see *infra* note 104 and accompanying text. Courts have struggled in particular with the circumstances under which a firm's loss of consumer data in a security incident can satisfy Article III standing requirements. *See, e.g.,* Nicholas Green, Note, *Standing in the Future*, 58 B.C. L. Rev. 287 (2017) (discussing standing in data breach litigation); Eric S. Boos et al., *Damages Theories in Data Breach Litigation*, 16 SEDONA CONF. J. 125 (2015) (same). This analysis was made even more difficult following the Supreme Court's recent holding in *Spokeo v. Robins*, in which the Court emphasized the need for harms to "actually exist" and to be "'real,' and not 'abstract'" in order to satisfy Article III's injury-in-fact requirements. *Spokeo v. Robins*, 136 S. Ct. 1540, 1548 (2016). Both the intangible nature of many cybersecurity-related harms, as well as remoteness of the harm from the underlying security incident, can make the "concreteness" of a given harm an indeterminate inquiry.

in violation of contractual assurances, but the court held that it did not represent a cognizable harm to the customers.[38] In that case, the court dismissed the lawsuit because the lack of awardable damages rendered it moot.[39] Similarly, courts have struggled with cases of identity theft or theft of credit cards, especially where credit monitoring services are provided to affected customers or banks refund fraudulent charges.[40] And even where courts are willing to recognize that harms are real, the question often turns back to questions of proximate cause. We live in a world in which information such as credit-card numbers is stolen with such frequency that it is difficult for a court to accept that fraudulent charges resulted from any specific theft of a consumer's information. It is simply too possible that the specific harm resulted from some other cyber-incident for the courts to award damages against a possibly innocent third party without some greater evidence tying the fraudulent use of credit-card information to a specific breach. Of course, such evidence is almost certainly impossible to gather.

There is another issue lingering in the background of the discussion so far. The sort of cases discussed above, in which a firm fails to properly protect its customers from adverse cyber-incidents, are governed by tort law, specifically negligence. Other forms of tort claims are similarly problematic.[41] But other issues are governed by contract law. Contract law is important in the cybersecurity context for two critical reasons. First, courts have generally upheld the use of contracts, including dense, boilerplate, consumer-facing contracts that are widely recognized as meaningless to consumers in the cyber-domain.[42] The contracts very often contain waivers of liability or other forms of indemnification.[43] Unfortunately, liability is typically contractually assigned away from parties that are most likely to be proven liable, or otherwise limits damages. This further compounds the problems of determining liability discussed above. Second, contractual language is often imprecise, a reflection of the complexity inherent in the cybersecurity ecosystem, which in many cases creates further uncertainty rather than clarifying responsibility.

Importantly, private law has a relatively simple mechanism for dealing with many of the difficulties discussed: strict liability. Under some

---

[38] *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 324–27 (E.D.N.Y. 2005).

[39] *Id.* at 326–27.

[40] *See* Amy Dunn, *Bridging the Gap: How the Injury Requirement in FTC Enforcement Actions and Article III Standing are Merging in the Data Breach Realm*, 20 J. CONSUMER & COMMERCIAL L. 9, 16–18 (2016) (describing the different approaches taken by courts in finding a basis for standing in cases involving threats of future harm).

[41] For example, intentional torts, such as trespass, are problematic because it is very difficult to identify the attackers, to attribute a specific attack to them, prove causation, demonstrate no contributory factors that offer the attackers a defense, and demonstrate cognizable, recoverable, damages.

[42] Scott, *supra* note 1, at 456.

[43] *Id.* at 457.

circumstances the law will assign liability to a given party regardless of fault. The canonical area of strict liability in tort law is products liability where the manufacturer of a defective product that causes consumer harm is liable for any harms caused by that product no matter how negligently the consumer was in its use.[44] For example, the manufacturer of a table saw would be liable for injuries caused to a consumer by a failure of the saw *even if* the consumer was using the saw for improper purposes—e.g., while intoxicated, after damaging the saw, and while wearing a blindfold and standing on crutches. Or, as another example, someone who chooses to engage in "ultrahazardous" or otherwise extreme activities like blasting with dynamite, or keeping dangerous animals like tigers as pets is generally subject to strict liability.

The underlying policy rationales for strict liability are discussed in Section III, which argues that cybersecurity should be a strict-liability regime. For the purposes of the present discussion, we need only say that courts have declined to treat services or computer software—the primary components of the cybersecurity ecosystem—as "products."[45] They therefore have not been treated subject to the rules of strict liability. Rather, they have been subject to the traditional principles of contract and negligence.

C. *Public Law Approaches to Cybersecurity*

There are various public law institutions in the United States that address cybersecurity issues. While some of these efforts effectively address narrow problems that effect parts of the cybersecurity ecosystem, there are no effective public law institutions that address broader problems. In particular, there are no public law institutions that generally ensure parties harmed by adverse cyber-incidents can secure recovery for their losses, that alter the perverse incentives faced by the various actors in the cybersecurity ecosystem, or that generally improve the overall quality of that ecosystem.

In the United States there is no general law of data security. Rather, there is a sector-by-sector approach to regulating specific security concerns. There are, for instance, specific laws and regulations relating to the security of financial information,[46] health information,[47] information about students,[48]

---

[44] Scott, *supra* note 1, at 457–58.

[45] *Id.* at 461–62.

[46] *See* Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106–102 (1999) ("An Act To enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, insurance companies, and other financial service providers.").

[47] *See* Health Insurance Portability and Accountability Act, Pub. L. No. 104–191 (1996) ("An Act To . . . improve portability and continuity of health insurance coverage . . . to combat waste, fraud, and abuse in health insurance and health care delivery . . . and for other purposes.").

[48] *See* 20 U.S.C. § 1232g (2013) (illustrating how the Family Educational and Privacy Rights Act (FERPA) controls the release of education records).

and consumer credit information.[49]

By and large, regulatory efforts to improve security such as these are inoffensive. Without question they draw additional attention and scrutiny to particularly sensitive areas and provide valuable resource towards the goals both of educating stakeholders about security concerns, and of taking action against those who fail to address these concerns. At the same time, we should be aware of the limitations of these targeted approaches. In almost every instance, sector-specific regulations are "consumer protection" statutes that impose controls on what information can be shared or used by those to whom it has been given. Firms generally implement these requirements by limiting how information they hold can be accessed by employees, or shared among their peers or partners. While this has the positive effect of protecting consumers, it has adverse effects of limiting the use of more efficient technologies or making more valuable uses of information. For instance, restrictions on the use and sharing of medical information dramatically hampers medical research; it is literally the case that some medical researchers believe such restrictions "threaten[] the social good by seriously restricting biomedical research and unnecessarily slowing the path toward life-saving discoveries."[50] Restrictions on financial transactions and disclosure of student records encourage firms to use outdated systems, impose burdens on consumers who need to authorize the disclosure or use of their information, and generally lead industry to make use of stale, but statutorily clear business practices instead of innovating new ones.

More problematic, because these rules are generally focused on protecting consumers, they are not focused on improving the overall state of the cybersecurity ecosystem. As such, they don't offer a systematic approach to addressing any of the issues that make cybersecurity difficult. Because these regulations are industry-specific, but the issues that make cybersecurity hard are generalized, none of the regulated industries are in a strong position to effect change to the broader cybersecurity ecosystem. Rather, each industry develops its own, costly, and largely inefficient (if not ineffective) means to protecting consumers.

The most direct federal "cybersecurity law" that Congress has adopted is the Cybersecurity Information Sharing Act of 2015 (CISA).[51] The purpose of this law is to immunize private firms from liability for sharing information relating to cybersecurity incidents with the government and, in some cases, other private firms.[52] Such information sharing is important to improving

---

[49] *See* 15 U.S.C. § 1681 (2013) (illustrating how within the Fair Credit Reporting Act (FCRA) credit reporting agencies must respect the consumer's right to privacy).

[50] ASS'N OF ACAD. HEALTH CTRS., HIPPA CREATING BARRIERS TO RESEARCH AND DISCOVERY, 1–2 (2008), http://www.aahcdc.org/policy/reddot/AAHC_HIPAA_Creating_Barriers.pdf.

[51] Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015) [hereinafter CISA].

[52] Larry Greenemeier, *A Quick Guide to the Senate's Newly Passed Cybersecurity Bill*, SCI. AM. (Oct. 28, 2015), https://www.scientificamerican.com/article/a-quick-guide-to-the-senate-s-newly-passed-cybersecurity-bill/.

cybersecurity, but there has been longstanding concern that firms that share such information could be subject to liability. CISA makes clear that "no cause of action [lies] against any private entity … for the monitoring or information systems and information" or "for the sharing or receipt of any cyber threat indicators or countermeasures" under the Act, and that "it shall not be considered a violation of any provision of antitrust laws for two of more private entities to exchange or provide cyber threat indicators, or assistance relating to the prevention, investigation, or mitigation of cybersecurity threats, for cybersecurity purposes under this Act."[53] The reality of CISA, however, is that it is a very small improvement coming more than a decade too late to meaningfully improve the cybersecurity ecosystem. CISA addresses concerns that were pressing in the early 2000s and which the private sector and federal government have already largely solved in the intervening years.[54] CISA reduces the friction involved with these solutions and provides firms a level of assurance that they are secure from liability that they did not have before. But the reality is that CISA was little more than a vehicle by which Congress could claim to have passed a "cybersecurity law."

Beyond CISA, the Federal Trade Commission (FTC) is the great exception to the sector-specific approach to cybersecurity in the United States. Since the turn of the century, the Commission has been working to use its general authority to regulate "unfair and deceptive acts and practices" under Section 5 of the FTC Act to establish itself as a general regulator of consumer-facing data security issues.[55] The FTC entered the business of regulating firms' data security practices largely in response to the failure of the private law described above. After courts began dismissing lawsuits because consumers could not establish harm, the FTC stepped in to take action against firms accused of mishandling consumer data, arguing that failure to protect consumer data was an unfair (or, if in violation of a firm's established security or privacy policy, a deceptive) business practice.

The FTC's efforts have been controversial, both lauded and criticized by many. Much of the controversy over the FTC's efforts relate to its use of broad and uncertain legal authority to regulate a large portion of the economy without clear Congressional authority to do so, and in particular its use of adjudication (as opposed to rulemaking procedures) to develop

---

[53] CISA 6(a), 6(b), 4(e).

[54] For instance, in 2003 DHS established the United States Computer Emergency Readiness Team (US-CERT) to coordinate information sharing across the federal government and with private sector actors. Greenemeier, *supra* note 52.

[55] *See* Justin Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955, 963–64 (2016) (citing Federal Trade Commission Improvements Act of 1980, Pub. L. No. 96-252, 94 Stat. 374 (1980) (codified at 15 U.S.C. § 57a (2012))).

binding legal norms.[56] What this means is that the Commission has not provided the industry with any formally issued guidance regarding what constitutes "good" or "bad" security practices. Rather, it has offered informal guidance on an occasional, often ad-hoc, basis, which it has sought to formalize by taking legal action against firms that, in the FTC's own estimation, are engaged in bad behavior. Due to the procedures the FTC has used in approaching this issue, the legality (and constitutionality) of this approach has not been addressed by the courts—though one case is currently pending that may lead to such a resolution.[57]

Regardless of the legality of the FTC's efforts to regulate data security practices, there are other reasons these efforts should raise concern. As an initial matter, the FTC approaches security from a consumer protection perspective. As such, and as with the sector-specific approaches, its efforts focus only on the outer border of the cybersecurity challenge. The FTC does not try, nor does it have statutory power to try, to address the myriad actors and mixed incentives that make ensuring cybersecurity difficult. It is possible that the FTC's approach will, over time, indirectly influence the incentives of the myriad actors in the broader cybersecurity ecosystem. As firms become increasingly aware that they may face liability for failure to protect consumer data, those firms may demand more secure systems from the rest of the ecosystem. This effect, however, will likely be largely muted in the case of the FTC's enforcement actions. As an initial matter, firms may choose, instead, to adopt clear policies indicating that consumers use their services at their own risk, or otherwise limit their liability. Indeed, on the FTC's own terms its efforts are only meant to hold firms to "reasonable" security practices, which should arguably be weighed in light of the current state of the art; these efforts therefore ought not to create any incentives to change the state of the art on their own.[58]

---

[56] *See id.* (discussing the FTC's reliance on administrative adjudication to develop a law of data security). For a more favorable take on the FTC's approach to data security, *see* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014); Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230 (2015); Chris Hoofnagle, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (Cambridge, 2016).

[57] *See* LabMD, Inc. v. FTC, No. 16-16270-D, 2016 WL 8116800, at *3 (11th Cir. 2016) (granting LabMD's motion for stay of FTC's order pending appeal). The few judges that have reviewed the case have implicitly or expressly expressed concern. Hurwitz, *supra* note 55, at 978.

[58] The precise meaning of "reasonable" as the FTC uses it in this context is unclear. In late 2015, an FTC Administrative Law Judge rejected an FTC complaint arguing that a medical testing laboratory's security practices were insufficient under the FTC Act. LabMD, Inc., No. 9357, 2015 WL 7575033 (F.T.C. Nov. 13, 2015) (dismissing the initial complaint). In June 2016, the FTC Commissioners overturned the ALJ opinion, finding that the firm's security practices were sufficiently lax to lead to a likelihood of consumer harm. LabMD, Inc., No. 9357, 2016 WL 4128215 (F.T.C. Jul. 28, 2016) (containing the final order). The case is currently on appeal to the Eleventh Circuit Court of Appeals. Pending the outcome of this litigation, the Eleventh Circuit has stayed the FTC's order, suggesting that the FTC's interpretation of the required "likeliness" of harm is insufficiently concrete (that is, that the

Another important problem with the FTC approach to cybersecurity is that it does not meaningfully inform or educate anyone about good security practices.[59] The primary audience for the FTC's data security is a small cadre of data security lawyers and information security professionals who work at relatively sophisticated, mid-to-large-sized, firms. This further insulates the effects of the FTC's efforts from the core cybersecurity challenges. First, to the extent that it is educating firms about good cybersecurity practices, the FTC is only communicating to those firms that already understand the challenges of cybersecurity, and that largely have the internal resources to address these challenges on their own. But the vast majority of online activity is undertaken by less sophisticated actors: consumers, small businesses, and start-ups, who either lack sophisticated understandings of, or the resources to address, cybersecurity challenges. And, importantly, these are the same actors who depend on outside resources, the myriad parties with mixed incentives that permeate the cybersecurity ecosystem, to educate and protect them.

III. STRICT CYBERLIABILITY

Section II explained that the law, when working well, can create powerful incentives that align individual conduct with socially-optimal goals, but that, in the case of cybersecurity, various factors confound the law's utility. This Section argues that a transition to strict liability for cybersecurity related harms would remedy the majority of these concerns, thereby allowing standard private law institutions to function and bring about dramatic improvements to the state of the cybersecurity ecosystem. In addition, this Section offers some suggestions for how to implement such a transition. Importantly, this is only the first part of this Article's broader recommendation. In Section IV I will turn to the desirability of a vibrant cybersecurity insurance marketplace in anticipation of Section V's discussion of the relationship between strict liability and the insurance marketplace.

A. *Defining Strict Liability*

The primary private law mechanism that has been used—or attempted, as described above—to address cybersecurity concerns is negligence. Under this model, parties are only liable for harms that they cause to others through

---

FTC interpreted "likely" to mean something equivalent to "merely possible," but that "likely" likely requires something more). *LabMD, Inc.*, 2016 WL 8116800 at *1, *3–4.

[59] Gus Hurwitz, *FTC's Efforts in LabMD Lack Required Due Process and Don't Actually Improve Security*, TECH POL'Y DAILY (Aug. 2, 2016, 6:00 AM), http://www.techpolicydaily.com/technology/ftc-labmd-dont-improve-security/; *but see* Hartzog & Solove, *The Scope and Potential of FTC Data Protection*, *supra* note 56.

their own negligence. In the classic formulation, a party engaging in an action that causes harm to someone else has acted negligently if the party failed to take precautions against such harms commensurate with the reasonably foreseeable likelihood and magnitude of those harms.[60] In other words, we expect people to take at least $50 worth of precaution to avoid a one in ten chance of causing $500 in harm to others.

The central idea behind the negligence model is that risk is unavoidable. Parties may be able to invest in mitigating risk, but cannot eliminate the possibility of risk entirely. If we were to hold parties responsible for any harm that they may cause to others, we are concerned that parties will over-invest in precaution or avoid risky but socially valuable activity. For instance, driving is inherently risky—on any given drive there is a chance that you will get into a costly accident. If we put too high a burden on drivers to avoid such accidents, they may over-invest in safety or avoid driving. But by only holding parties responsible for taking reasonable precautions—that is, those commensurate with foreseeable harms—we do not dissuade any socially beneficial activities. In other words, modern negligence liability is designed to ensure that parties engage in the socially optimal level of activities.

But negligence is not the only approach to assigning liability. Starting in the 1960s, courts began to impose so-called strict liability in some cases.[61] Under a strict-liability regime, a given party is always responsible for the harm incurred by its counterparties, no matter how careful that party was to avoid such harm.[62] The underlying theory is that one party may be in a better position to prevent or assess the likelihood of certain harms than the other. An important situation where this is the case is where assigning liability to one party allows for risk pooling. For example, parties on one side of a transaction systematically may not be able to absorb costs, or the expected costs may be distributed too thinly to justify taking precautions. It is also the case where one party is in a better informational position than the other, or is in a better position to gather or disseminate information.

Counterintuitively, as will be considered further in Section V, strict liability does not affect the level of care that a party will take. One intuitively expects that if we impose strict liability on a party, that party will take greater precautions to avoid such harms than if it would only be liable in the event of its own negligence. This is not the case. Under either model, parties will

---

[60] *See* United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947) ("[T]he owner's duty, as in other similar situations, to provide against resulting injuries is a function of three variables: (1) The probability that she will break away; (2) the gravity of the resulting injury, if she does; (3) the burden of adequate precautions.").

[61] *See infra* Section III.C (containing case law regarding strict-liability standards for tort law).

[62] *See* Richard A. Epstein, *A Theory of Strict Liability*, 2 J. LEGAL STUDS. 151, 168 (1973) (stating that under strict liability, "a party who has caused a loss must pay damages whether or not he was negligent"); Shavell, *supra* note 3, at 127–28 (discussing coverage and premiums related to liability insurance).

only invest in avoiding harms up to the point that the cost of such investment is commensurate with the expected magnitude and likelihood of harm. In other words, it never makes sense to spend $75 to mitigate a one in ten chance of causing $500 in harm. Rather, under strict liability, one will spend $50 in precaution and simply pay the balance of $450 if that $500 in harm happens to occur. The key difference between negligence and strict liability is how the $450 loss that results when the harm does occur. Both negligence and strict liability accept that bad things happen and that no amount of precaution can prevent every risk. In fact, we do not want people to invest in inefficient levels of precaution. The difference between the two systems is that in a negligence regime, the harmed party bears the cost of the harm. Contrastingly, in a strict-liability regime, it is borne by the other party. While the strict liability model may seem grossly unfair, we will see in Section IV that it turns out to function much like an insurance system and that it can be a very positive model in some circumstances.

B. *No Strict Cyberliability Today?*

At this juncture, the point must be clearly made that software and computer systems historically have not been subject to strict liability and, absent statutory intervention, are not likely to be made subject to strict liability. In the modern tort setting, strict liability applies almost exclusively in the context of products liability. Over the past several decades, courts have struggled to fit computer software within the ambit of products liability. They have struggled to determine whether software is a "product"; they have struggled over whether inadvertent software errors rise to the level of defective design; and they have struggled with whether software released without sufficient testing to avoid errors is defectively manufactured.[63] Indeed, because software is generally not viewed as a "product," and because it is generally licensed under copyright law, courts have generally found any contractual and license terms pertaining to the sale or license of software to be enforceable—and these terms almost always include disclaimers and waivers of liability.[64]

Even if we view software as a product and software defects as design or manufacturing defects, there are still challenges to applying strict liability for software. For instance, we still face difficulties in establishing damages

---

[63] *See* Scott, *supra* note 1, at 430–35 (discussing whether software is a product).

[64] *See* Jennifer Chandler, *Information Security, Contract and Liability*, 84 CHI.-KENT L. REV. 841, 843 (2010) ("Yet, the purchasers of software are usually contractually bound by end user license agreements . . . which contain generic disclaimers about fitness, functionality, or quality, as well as exclusions of liability exempting the vendors from any problems that arise from defects.").

and recovery may be limited by the economic loss doctrine.[65] And an even greater challenge to bringing a "strict" products liability claim is that courts have increasingly embraced what is known as the risk-utility test to determine products liability.[66] Under this approach, products liability takes on a very negligence-like characteristic.[67] 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.[68]

Over the years, there have been frequent calls for the application of strict products liability principles to computer software.[69] Nonetheless, the status quo today is that defective software today is only subject to liability under principles of ordinary negligence, if at all.[70]

C. *Cybersecurity is a Classic Case for Strict Liability*

Despite the discussion above, cybersecurity presents a near textbook case for strict liability. The policy rationales for strict liability—the challenges that strict liability evolved to address—match the challenges created by cybersecurity. Indeed, even the historical challenges that gave rise to modern strict liability map onto the issues faced today in the cybersecurity setting. And while there are a number of common concerns about strict liability—concerns that militate against its use in various settings—they are largely inapposite to the cybersecurity setting. The discussion below turns away from the application of the legal rules that surround strict liability today and focuses instead on the historical development of the doctrine and the economic understanding of how it functions.

---

[65] *See* Opderbeck, *supra* note 35, at 982 ("The suggestion that data breach tort claims should not be barred by the economic loss doctrine does not affect the issue of the need to prove ascertainable losses in order to have Article III standing.").

[66] *See* Scott, *supra* note 1, at 467–68 (defining the risk-utility test).

[67] *Id.* at 467.

[68] *See, e.g.*, Lorin Brennan, *Why Article 2 Cannot Apply to Software Transaction*, 38 DUQ. L. REV. 459, 508 (2000) ("To argue that a software publisher is obligated to disclose all 'defects' in a program begs the enormously difficult issue of defining just what a software 'defect' is, let alone the computational difficulties of determining what every defect might be."); Daniel Garrie, *The Legal Status of Software*, 23 J. MARSHALL J. COMPUTER & INFO. L. 711, 736 n. 167 (2005) ("One major impediment to the application of strict liability is the widely held belief that it is virtually impossible to guarantee that software is error-free"); Sheldon Childers, Note, *Don't Stop the Music: No Strict Products Liability for Embedded Software*, 19 U. FLA. J.L. & PUB. POL'Y 125, 172 (2008) ("If it is impossible for the average developer who relies on these ever-changing tools and technologies, through reasonable effort, to completely eliminate defects from software, it follows that embedded software is to some extent unavoidably unsafe. … As applied to software, strict products liability would attempt to compel a result over which the software engineer lacks control.").

[69] Scott, *supra* note 1, at 467. Perhaps the most poignant, and prescient, of these calls, was made by Danielle Citron in *Reservoirs of Danger*, *supra* note 1.

[70] *See supra* Section II.B.

1. *The Origins of Strict Liability*

The origins of modern strict liability in the American legal tradition are generally traced to Judge Cardozo's famous opinion in *MacPherson v. Buick Motor Company*,[71] which eliminated the privity requirements for suits brought in tort.[72] Prior to *MacPherson*, individuals could only bring suit against those with whom they shared some direct connection (that is, with whom they had privity). In other words, if a driver were injured in an automobile accident caused when a component of her car failed, she could only sue the person who sold her the car—she could not sue either the car manufacturer or a third-party manufacturer of the component that failed (for instance, if the component that failed had been bought by the manufacturer and integrated into the final component, as is often the case with many automotive components, such as tires). All of these parties only have an indirect relationship with the driver, so are said to lack privity. Under the pre-*MacPherson* model, the driver would be expected to sue to person who sold her the car and that person could then countersue other third parties, either under separate legal theories or seeking indemnification.

MacPherson changed all of this, opening the door to direct suits by drivers (or other end-users) against manufacturers (or other responsible parties in the supply chain). The underlying rationales were intended to address the same sort of challenges that we see in the cybersecurity context. The multiplicity of parties in a supply chain make it difficult to figure out who to sue and make it difficult to establish or apportion liability. In both the case of *MacPherson* and the modern cybersecurity setting, this effectively externalizes risk onto consumers, and creates perverse incentives for how the various entities through the relevant product ecosystems design their products and services.

MacPherson was only the first step towards the modern understanding of strict liability. While it allowed parties to bring suits in the absence of privity, those suits were still brought under a negligence standard. Starting in the 1960s, some courts began developing the modern understanding of strict liability in cases involving consumers harmed by (arguably) defectively designed or manufactured products. The canonical case is *Greenman v. Yuba Power Products*,[73] which involved a wonderfully monstrous power tool sold by Yuba, the "Shopsmith, a combination power tool that could be used as a saw, drill, and wood lathe."[74] Mr. Greenman was injured a year or so after his wife purchased Shopsmith for him as a

---

[71] 111 N.E. 1050 (N.Y. 1916).

[72] *See id.* at 1053 ("We have put aside the notion that the duty to safeguard life and limb, when the consequences of negligence may be foreseen, grows out of contract and nothing else.").

[73] 377 P.2d 897 (Cal. 1963).

[74] *Id.* at 898.

Christmas present, and brought suit for breach of warranty and negligence.[75] The trial court determined that the manufacturer had not been negligent, and that Mr. Greenman's harms were not covered by any express or implied warranty.[76]

On appeal, the Supreme Court of California found the manufacturer strictly liable for Mr. Greenman's injuries, explaining that the question of "liability is not one governed by the law of contract warranties but by the law of strict liability in tort."[77] As explained by the court, "[a] manufacturer is strictly liable in tort when an article he places on the market, knowing that it is to be used without inspection for defects, proves to have a defect that causes injury to a human being.[78] "The purpose of such liability is to insure that the costs of injuries resulting from defective products are borne by the manufacturers that put such products on the market rather than by the injured persons who are powerless to protect themselves."[79] Critically, under a strict liability model, parties are not free to assign risk of harm by contract—any contract or warranty attempting to do so is a legal nullity.

2. *Strict Liability and Negligence*

Strict liability is an exception to the ordinary rule of negligence—it is only used in certain cases. The traditional examples are products liability, such as was the case in *Greenman*, and so-called ultrahazardous activities, such as keeping dangerous animals as pets or the use of explosives.[80] It is clear why we only turn to strict liability in cases like these—and why cybersecurity is a similar case—when we look to the core policy rationale underlying strict liability: ensuring that liability for harms be assigned to parties best able to bear it. Both negligence and strict liability accept that some amount of harm naturally occurs in the world. Under a negligence model, we assume that parties bear, and are able to bear, comparable responsibility for preventing or accepting the risk of harm. Under strict liability, we assume that the parties—especially in their abilities to prevent or accept risk—are asymmetric. In terms of preventing risk, we are generally concerned about risks that would be unreasonably, or impossibly, costly for individuals to detect. For instance, if a consumer could not determine whether a saw blade contained manufacturing defects without engaging in

---

[75] *Id.*

[76] *Id.* at 898–99.

[77] *Id.* at 901.

[78] *Id*. at 900.

[79] *Id*. at 901.

[80] RESTATEMENT (SECOND) OF TORTS § 519 (AM. LAW INST. 1977) ("One who carries on an abnormally dangerous activity is subject to liability for harm to the person, land or chattels of another resulting from the activity, although he has exercised the utmost care to prevent the harm."); *id.* at § 520 cmt. g ("If the potential harm is sufficiently great, however, as in the case of a nuclear explosion, the likelihood that it will take place may be comparatively slight and yet the activity be regarded as abnormally dangerous.").

destructive testing of the blade, the law may hold the blade's manufacturer strictly liable for manufacturing defects. Similarly with ultrahazardous activities, where it is unreasonable, for instance, to expect individuals to take precautions against the use of explosives in construction operations or pet tigers that may be roaming the streets, we place a strict burden on the party engaging in the atypical activity. We see the same in terms of accepting risk. In this case, the concern relates to the parties' relative abilities to bear the costs of a risk should harm come to pass. Again, the example of an injury related to power tools is illustrative: such an injury could be physically or economically devastating to an ordinary consumer, and many consumers do not have the knowledge or wherewithal to insure against such losses. The manufacturer, on the other hand, is in a much better position to assess the possible risks, and to insure consumers against those risks.

This rationale for strict scrutiny is not without criticism or nuance. Many of the criticisms of, and concerns raised by, strict-liability regimes will be considered shortly below—and the idea that strict liability acts as a form of insurance will be considered in greater depth in Section V.

3. *Strict Liability and Cybersecurity*

Before considering these issues, we can outline the case for applying strict liability in the cybersecurity context. We already saw that the rationale for the first steps towards strict liability—*MacPherson*'s abandonment of privity requirements[81]—mirrored concerns similar to those we see in the cybersecurity context: the difficulty of attributing liability and recovering damages that results from the multiplicity of actors and the complexity of their interconnected relationships. So, too, do the concerns about parties' relative abilities to prevent and accept risk motivate modern principles of strict liability mirror reality of the cybersecurity setting. As discussed in Section I, every entity engaged in conduct online—from individuals, to small businesses, to non-profit and governmental organizations, to large non-tech firms, to large tech firms—is exposed to cybersecurity risks. Mitigating these risks is far beyond the expertise of the vast majority of these entities. And, even if it were not beyond their expertise, most defects in third-party systems are latent. Even if these third parties open their systems up for inspection, it is functionally impossible to expect even sophisticated parties to audit them for defects at reasonable costs.

This is largely descriptive of the situation that exists in the business-to-business landscape. Even among sophisticated parties, few are in a position to meaningfully understand, let alone prevent, cybersecurity risks. But this is even more dramatically the case in the consumer-to-business relationship. Here, consumers are almost entirely at the mercy of the firms they interact with online to keep data that they disclose to those firms secure. Consumers

[81] MacPherson v. Buick Motor Co., 111 N.E. 1050, 1053 (1916).

have no visibility into those firms' systems, into what data those firms retain, how they manage that data or use it, or to whom it is disclosed (intentionally or unintentionally). Once their data has been shared with a firm, consumers have literally no ability to monitor its subsequent use or handling, to take precautions to prevent harm, to detect its misuse, or to take action in response to those harms.

Indeed, the cybersecurity context arguably presents a more "textbook case" for the use of strict liability than seen in most "textbook cases." Strict-liability regimes have two basic effects: they increase the price of products and services and they encourage risk-taking by consumers. They increase the cost faced by providers of products and services because those providers bear the risk of any liability. But these costs are almost always passed on to consumers. The net effect, discussed in more detail in Section IV, is that firms subject to strict liability act as insurers: they spread the cost of risk across the entire pool of consumers, collecting a premium for that risk through the price they charge, and they use those premiums to pay out damages as they occur on a stochastic basis. Importantly, the concern about increasing prices has an important, potentially pernicious, secondary effect: more price sensitive consumers, or those who are less exposed to risk, may select themselves out of the market. This has the effect of spreading the cost of risk across smaller pool of consumers, each of whom therefore has to pay proportionally more. Taken to the extreme, this can make some products unviable in the market—as was indeed observed in the 1980s.[82] In proposing a strict-liability regime, we need to be very cautious about this concern, as it could be devastating to the market. The second concern is similarly important: if consumers are aware (implicitly or explicitly) that another party is liable for any harm that befalls them, consumers may have an incentive to opportunistically engage in riskier behavior. For instance, consumers may shirk on routine maintenance of potentially dangerous products, or fail to read manuals or otherwise educate themselves to the safe operation of potentially dangerous products, if they know that they will receive compensation despite their own negligence.

4. *Challenges of Strict Liability*

There are two well-understood problems raised by strict liability: adverse selection and moral hazard.[83] Fortunately, neither of these concerns is substantial in the cybersecurity context. Users and purchasers of products and services throughout the cyber-domain consistently have little ability to control, monitor, or prevent against harm. At the retail level, consumers are

---

[82] Priest, *supra* note 3, at 1521.

[83] *See* James R. Garven, *Moral Hazard, Adverse Selection, and Tort Liability*, 28 J. INS. ISSUES 1, 4, 6–7 (2005) (explaining the effect of compensation from moral hazard and adverse selection); *see also* Tom Baker, *On the Genealogy of Moral Hazard*, 75 TEX. L. REV. 237, 238–40, 285 (1996) (further defining moral hazard in comparison to adverse selection).

wholly at the mercy of the firms with which they work and to which they provide data to ensure that that data is reasonably stored, used, and secured. The best that even a sophisticated consumer can do is rely on a firm's assurances and reputation. But if the past several years have demonstrated anything about security, it is that even security-conscious, sophisticated firms can be the subject of cyber-incidents. The same also holds in the business-to-business context. When one firm engages another to provide security related services or products, it is generally because the contracting firm lacks the sophistication or resources to implement those products or services on its own. And, as discussed at the beginning of this Article, the complexity of software and of designing secure systems, means that contracting parties cannot reasonably audit or monitor the performance of most security-related products or services.

Taken together, this analysis means that neither of the common concerns about strict-liability regimes apply in this context. A transition to strict liability likely will increase the cost of providing products or services, especially in the short run, but not in a way that is likely to adversely affect consumers. The risk of harm from cyber-incidents is spread relatively uniformly across the online ecosystem, which means that we are not worried about price increases causing some portion of the market to opt out of the market (leading to further increases in price to the remaining portion). Indeed, the opposite is more likely to occur: concerns about security today increase the cost of participating in these markets today, which may cause risk-averse users to opt out of the market (or to engage in costly and largely ineffective self-help, such as using complex password management systems or multiple e-mail addresses). Pushing the cost of these risks back to the parties best able to mitigate and bear them could actually grow the market, rather than segmenting it. And, in the long run, placing the risk of cyber-incidents on parties that are better able to mitigate them will likely lead to an overall improvement in the systems that make up the cybersecurity ecosystem, reducing the overall risk for everyone. Similarly, the second concern about strict liability—that, in this context, it creates perverse incentives for users and contracting parties to engage in riskier behavior—is largely inapposite. Today, it is hard to imagine an environment in which participants routinely engage in riskier behavior.

The basic problem in the security ecosystem as it exists today is that the difficulty of imposing liability in negligence and contract models has effectively created a "strict fault" regime. Under this current regime—which is governed by negligence and contract law in name only—sophisticated parties pervasively externalize risk upon unsophisticated parties. This is exactly the opposite of how the law usually works, and of how we should want to see incentives structured: we generally want to impose liability in the first instance on the parties best able to prevent harm from occurring or to absorb the risk of harms that do come to pass. Doing so tends to reduce

overall risk to society by maximizing incentives to efficiently reduce it and minimizing the costs to those dealing with it. Under a negligence and contract model, we have seen the opposite: incentives to burden unsophisticated parties with risk rather than working to mitigate it, without any concern for the cost of the resulting harms. Strict liability is manifestly a better approach.

D. *Limitations: Statutory Damages, Other Practicalities, and Best Laid Plans*

Transitioning to a strict-liability regime would address many of the problems facing today's cybersecurity ecosystem—an argument taken up in Section V. But strict liability is not a panacea. Before turning to discussing the relationship between strict liability and insurance, some practicalities of implementing a strict-liability regime for cyber-incidents need to be considered.

The substantial limitation on a strict-liability regime is that it does nothing to address the question of damages. Recall that one of the greatest obstacles to imposing civil liability on firms that have experienced data breaches, or other cyber-incidents, has been proving cognizable harm in court. Courts have consistently found that damages cannot be awarded in these cases because causation is too tenuous, there are too many potential intervening factors that could have caused any harm, or harm is too speculative to quantify.[84]

There is a straightforward solution to this problem: statutorily directed damages. "Statutorily directed" means two things. First, courts should be instructed to err on the side of finding cognizable damages. Evidence still needs to be required to support a finding of damages, but courts can be statutorily directed to require a reduced burden of proof, shift the burden of proof, or accept that certain harms (e.g., privacy harm) are cognizable. Second, and more important, Congress can direct the establishment of a schedule of damages to be used by courts in establishing damages for various sorts of harms at trial. The FTC, for instance, could be directed to establish such a schedule of damages through a rule-making process, with instruction that the schedule be based on empirical data but that the agency should err on the side of finding substantial damages and that deference should be given to the agency in interpreting that data. Indeed, it may make sense to require the agency to use a multiplier in setting damages. Once such a schedule of damages had been set, courts would use it as a floor in the civil context—a judge could still find higher actual damages or assess punitive damages where appropriate—and would otherwise fall back on the statutory direction to find cognizable damages in the event of harms not covered in

[84] *See supra* note 37 and accompanying text; *see also* Opderbeck, *supra* note 35 (discussing various challenges that face cybersecurity related litigation, focusing on the economic loss doctrine).

the schedule.

There is also a question of who would be subject to strict liability in the cybersecurity context, given the multiplicity of actors in the ecosystem. The policy rationale for applying a strict liability rule do not apply across all of the relationships in this ecosystem. At one extreme, system vendors and integrators and their clients are often sophisticated parties engaging in negotiated commercial contracts. There is little reason that these parties should be subject to anything other than the contractually negotiated terms of their contracts. On the other extreme, as discussed above,[85] consumer-facing firms providing services to and collecting information from consumers present a near-classic case in which strict liability is appropriate.[86] Any cybersecurity related strict liability rule should be designed to apply only to those firms where principles of ordinary negligence or contract law do not sufficiently protect parties from security related risks.

Beyond the question of damages, there are other implementation details and decisions that would need to be addressed. A few specific points are discussed below, with the goal of designing a system that is broadly incentive aligned—though it is certainly not the only approach, and there certainly are other issues that may need to be addressed. One challenge that the switch to strict liability does not address is the incentive that firms face to detect, disclose, and otherwise respond to adverse cyber-incidents. Simply stated, under any liability regime a firm will face no liability if it can keep an incident secret. As an initial matter, a federal civil cause of action should be created alongside the transition to strict liability that allows both private parties (acting alone or as a class) and the FTC to bring civil actions in federal court. The low bar to recovery created by the strict liability nature of this cause of action, along with the multiplier to be used by the FTC (or other agency) in developing a schedule of damages, creates an initial incentive for those potentially harmed by cyber-incidents to be vigilant in monitoring and taking action in response to them. Additionally, punitive damages should be expressly authorized—even encouraged—for firms that do not timely detect or respond to a cyber-incident. On the other hand, firms should be affirmatively encouraged to put procedures in place for the timely detection of and response to cyber-incidents—including providing notice and reasonable compensation to harmed parties. One simple approach to creating such an incentive is to bar suits by the FTC or class actions against firms that have such procedures in place.

---

[85] *See supra* Section III.C.

[86] Similarly, firms that collect or aggregate consumer information without any direct involvement from consumers also present a strong case for strict liability. *See supra* Section III.C.3.

IV. CYBERINSURING LIABILITY

Section III of this Article argued the merits of using strict liability to address harms that result from cyber incidents. Use of strict liability in this context would correct many of the challenges that parties face in establishing liability for harmful conduct discussed in Section II. In particular, the failures of existing private and public law mechanisms to assign liability for cyber-incidents creates incentives for those who would otherwise bear the cost of mitigating or the costs of harms caused by such incidents—generally the same parties who are in the best position to take precautions against them—to externalize the risk of cyber-incidents on to third parties—generally those least able to mitigate or afford to bear such risk. In effect, the current model is a no-(third-party)-liability model, which creates pervasive, harmful incentives. Adopting a strict liability model would go far to align public and private incentives to reduce cyber-incident risks to a more efficient level.

It turns out that there is a nexus between strict liability and the sort of insurance that would improve the state of cybersecurity. Academics have been discussing the value of cyber insurance as a mechanism for improving the overall state of cybersecurity for over a decade, but in more recent years have lamented the insurance marketplace's failure thus far to realize this possibility.[87] Indeed, while the cyber-insurance marketplace has grown substantially in recent years, the policies that are being written are largely structured in ways that limit the broader impact of insurance on the state of cybersecurity. In order to improve the quality of cybersecurity, insurance needs to provide more complete coverage—in particular, insurers (and, through them, the rest of the ecosystem) need to internalize the risks that are systematically externalized due to the diffuse nature of the cybersecurity ecosystem. It turns out that strict liability, in economic terms, actually is a form of insurance, and as a form of insurance it is particularly sensitive to these externalized third-party effects.

This relationship between strict liability and insurance, and potential effects on cybersecurity, is discussed in Section V. Before turning to that discussion, this Section provides a background discussion of insurance generally and of cyber insurance in particular. It starts by providing a general overview of what insurance is, its potential applicability in the cybersecurity context, and its limitations.

---

[87] See, e.g., Kesan & Mullins Hayes, *supra* note 2 (noting that only about a third of U.S. firms carry cyber-insurance policies and that commercial general liability policies often exclude, and carriers litigate to narrow coverage of, losses related cyber-incidents); Singer, *supra* note 2, at 7 (noting that cyber insurance "is a drop in the bucket compared to the overall scale of the insurance industry . . . the scale of our digital economy, and the scale of cybersecurity risk . . . .").

A. *Defining Insurance*

1. *Risk Pooling*

Insurance is tool for pooling risk.[88] It allows parties that face predictable but uncertain risks to reduce the variance in costs that they face as a result of the risks. It is driving by the statistical "law of large numbers," which tells us that if we take a large number of parties that face similar risks, on average each party will incur the average costs of these risks. In other words, if 100 parties face a 10% chance of a $1,000 loss and a 90% chance of a $0 loss, each of those parties will experience an average loss of $100.

Without insurance, a party subject to this risk will either incur no loss or a $1,000 loss—it will never incur the average, $100 loss. Such a party is said to self-insure: it will face a $1,000 liability should the risk of loss materialize and so must be in a position to pay out that much. Such a party is also said to face a large variance in expected outcomes: it will pay out either $0 or $1,000.

With insurance, the insured party will pay an insurer the average expected loss amount ($100, plus some administrative fee to cover the insurer's costs). Should the risk materialize, the insurer will pay out $1,000; should it not materialize, the insurer keeps the $100. A party buying such an insurance policy faces small variance: it knows that it will pay exactly $100 in all circumstances. This provides the insured with predictable and stable flow of costs.

Insurance does not necessarily reduce or eliminate risk. Rather, it transfers it from the insured party to the insurer. By pooling risk from a large number of insureds, insurers are in a better position to absorb the costs of risk. When a risk materializes into an actual liability, the costs on a self-insuring party can be substantial. This is immediately intuitive to most people: the sudden imposition of tens or hundreds of thousands of dollars that can result from even a non-catastrophic car accident could easily bankrupt most drivers. But, thanks to the law of large numbers, an insurer who insures a sufficiently large number of parties can anticipate and manage its cash flow to accommodate such losses.

2. *The Actuarial Process: First- and Third-Party Insurance*

The heart of the insurance businesses is the actuarial and underwriting process. This is the process by which insurers identify and estimate the likely costs of the risks that a party wants to insure against. For instance, a driver will provide insurers with demographic information, information about her car and driving record, her driving patterns, and the like. A successful insurer will accurately estimate these risks and their associated costs and charge its insureds a concomitant amount.

---

[88] THE WORLD BANK & GAVI ALLIANCE, BRIEF 4: RISK-POOLING MECHANISMS 1, 4 (2010), http://apps.who.int/immunization_financing/tools/Brief_4_Risk-Pooling.pdf [].

On the other side of this process, the party seeking insurance needs to identify what risks it wants to insure against. There are a number of standard risks for which we use insurance: automobiles, unemployment, health care, loss or damage to houses or businesses, and the like. In principle, insurers are generally willing to sell insurance against *any* risk, provided that they can reasonably estimate the likely risks and costs of loss—though, in cases of indeterminate or particularly costly, likely losses, premiums for such policies can be substantial.

A particularly important distinction in types of insurable risks is that between first-party and third-party liabilities. Most insurance is first-party, meaning that when the insured party experiences a loss, insurance compensates it for those losses. In third party insurance, the party purchasing the insurance is doing so to insure a third-party against loss. For instance, a firm seeking to do business that may cause risk to third parties may agree to purchase insurance to insure those parties against that risk—sometimes even without those third-parties' knowledge.

3. *Insurance as Regulation*

Most insurers are not passive entities. They make money by reducing the actual rate of loss compared to the actuarially anticipated rate of loss. There are a number of ways that this can be accomplished. A primary function of the underwriting process is not only to assess the actuarial risks of a potential insured, but to educate and instruct the insured on how to reduce those risks. In some cases, this is an entirely passive process. For instance, an automobile insurer is likely to indicate to potential customers that there are discounts for drivers of cars with airbags, anti-lock brakes, or other safety devices; and drivers who have completed driving safety courses are also likely to pay lower premiums. The primary purpose of these discounts is to determine a driver's actuarial risk—but by announcing them, drivers are also educated about ways to reduce their risk. In other cases, this process is more active. For instance, a business seeking insurance against theft is likely to go through a more intensive underwriting process that will involve an actual inspection or in-depth checklist of the business's security practices and that will identify egregious risks (and likely insist that they be addressed prospectively) and will include express directive guidance on best practices.

In other cases, insurers may attempt to improve actuarial risks for all of their actual or prospective clients—instead of focusing on individual customers in the underwriting process. Perhaps the best example of this is the lawsuits filed by automobile insurers in the 1980s to challenge the decision by the National Highway Traffic Safety Administration (NHTSA)

to stop requiring cars to come standard with seat belts.[89] Of course, insurers do not do this out of the goodness of their hearts; they do so because it is likely to increase their profitability. This is particularly likely to be the case where the use of insurance is required (expressly or implicitly) by law, where parties subject to the insured risk are unlikely to appreciate the potential costs of the risk, or where the actuarial costs of insurance are high enough to push a significant number of firms out of the market. As we will see below, all three of these are likely to be the case with cyber insurance.

B. *The Virtues of Cyber-insurance*

Insurance can have a broad regulatory effect on a market, improving both the conduct of those using insurance and the overall state of a given market. Insurers have unique abilities and incentives to inform firms of their legal obligations, to develop best-practices, to audit and educate firms as to those practices, and to lobby for improvements to the overall state of the cybersecurity ecosystem. For this reason, widespread adoption of cyber insurance would potentially spur dramatic improvements in quality of the cybersecurity ecosystem.

Section I of this Article made the case that, stated simply, cybersecurity is hard. Participants throughout the cybersecurity ecosystem have surprisingly little understanding of the pervasive risks and challenges associated with cybersecurity, let alone an understanding of best (or even merely good) practices. At the user level, individuals rarely have familiarity with principles of security "hygiene," as it is referred to in the literature—concepts like how to identify and respond to risks, how to manage passwords, e-mail accounts, and other sensitive information, and with whom to share or not share information. Going up a level in the food chain, small businesses frequently lack all of this knowledge as well but are also tasked with bigger, more complicated challenges: how to design and secure basic IT systems, how to monitor, identify, mitigate, and respond to cyber-incidents, how to design and implement an incident response plan. For most small- and even mid-sized businesses, it is enough of a challenge (and expense) just to get a basic IT infrastructure in place. Especially outside of the tech sector, most firms don't even know what issues they face, let alone how to address them. The same basic story can be told at nearly every level of participation and sophistication in the cybersecurity ecosystem; even those who are implementing systems often lack information about the needs and sophistication of their customers, making it difficult to design systems that promote good security hygiene.

---

[89] *See* Tom Baker & Rick Swedloff, *Regulation by Liability Insurance: From Auto to Lawyers Professional Liability*, 60 U.C.L.A. L. REV. 1412, 1423 (2013) (discussing the factors that affect claims in lawsuits, like "airbag and seatbelt regulation").

Insurance—and insurers—are uniquely situated to address these system- and ecosystem-level concerns.[90] The basic business of insurance is the collection of data relating to risk, the quantification of that risk, the evaluation of individual insureds' risk profiles, and the minimization of both their insureds' exposure to and the overall market's creation of risk.[91]

An insurer's first job is to build its actuarial tables—to collect data that will allow it to evaluate an individual insured's exposure to risk in a given industry. This is a process that, in the context of cybersecurity, we will return to in Section V.

Once an insurer has a sense of the factors that go into determining an individual insured's exposure to risk, it can begin underwriting new clients. This is the process by which insurers evaluate possible clients' risk profiles to determine their insurability and the premiums to be charged for insurance. In the cybersecurity context, for instance, an insurer is likely to conduct an audit of a firm's systems and procedures: what is the architecture of the firm's network, what data is stored and used, how is access controlled, what incident response plans are in place, how are employees trained and monitored, how is third-party access to the firm's systems (e.g., by contractors) assigned and monitored, and the like. This process alone offers—or would offer—most firms a more in-depth evaluation of their cybersecurity systems than they would ever otherwise receive, except possibly in the case of a serious security incident. Even more important, it would offer these firms the most in-depth education regarding security best-practices that they are likely to ever receive. Moreover, insurers have an incentive to monitor their insured's ongoing performance, providing ongoing updates and training regarding best practices and responses to newly discovered security problems

It is difficult to imagine a more effective approach to educating and evaluating the bottommost layers of the security pyramid. And this leads to a second powerful benefit of widespread adoption of cyber-insurance policies, effective push-back against the pervasive externalization of risks from sophisticated parties onto unsophisticated parties. There are two sources of this push-back. First, as consumers and firms are informed by insurers about their exposure to risk, they will have greater demand for more secure products. This means both that they will be willing to pay more for more secure products (which would lower their insurance premiums), and they will put greater pressure on vendors and service providers to provide

---

[90] For some of the best treatments on the role that insurers can play as regulators, *see* Omri Ben-Shahar & Kyle D. Logue, *Outsourcing regulation: How Insurance Reduces Moral Hazard*, 111 MICH. L. REV. 197 (2012); and Tom Baker, *Liability Insurance as Tort Regulation: Six Ways that Liability Insurance Shapes Tort Law in Action*, 12 CONN. INS. L.J. 1 (2005). *See generally supra* note 2.

[91] *How Insurance Works*, INSURANCE INSTITUTE MICH. (2010), http://www.iiminfo.org/CONSUMERS/HowInsuranceWorks (discussing the procedures of how insurance is priced, sold, and purchased).

more secure products and services. And second, the insurance industry itself will serve as a powerful lobby to push for better designed and more secure products and services. The software and tech industries are powerful interests that have largely been successful in shielding themselves from liability for the quality of their wares—for good reasons and bad. There is no concerted interest group on the other side of this balance—consumers are too diffuse a group with too little an understanding of the relevant harms to which they are exposed to effectively lobby against Silicon Valley or the Business Software Alliance to demand risk be shifted back to those who have built the insecure infrastructure on which we have come to depend.

C. *Limitations of Cyber-insurance: Damages, Data, Exposure, Externalities*

Despite the positive story about cyber insurance told above, the reality of the cyber-insurance market is less rosy. The cyber-insurance market faces a number of challenges. While it has been growing at a substantial pace in recent years, it is still "just a drop in the bucket" compared to the scale of the cybersecurity problem.[92] As recently noted by Peter Singer, less than half of Fortune 500 firms have cyber insurance; 18,000 mid-size firms do not have cyber insurance; and only 5% of manufacturing firms have cyber insurance.[93] Overall, only about a third of US firms carry cyber insurance policies.[94]

In recent years, academics have extensively studied the incentives that insurers have to offer cyber insurance.[95] The particular focus of these studies has been to determine whether insurers are likely to offer policies that will improve the overall quality of the cybersecurity ecosystem. The general conclusion has been that they do not.[96] Except in the case of a monopoly

---

[92] Singer, *supra* note 2, at 7.

[93] *Id.*

[94] Kesan, *supra* note 2.

[95] *See, e.g.*, Podolak, *supra* note 2, at 399 (discussing the types of coverage insurers may offer); Christian Biener et al., *Insurability of Cyber Risk: An Empirical Analysis*, 40 J. GENEVA PAP. RISK INSUR. ISSUES PRACT. 131, 148 (2015) (discussing factors that insurers consider before offering cyber insurance); Lelarge & Bolot, *supra* note 2 (analyzing the risks and rewards that insurers face in offering cyber insurance); Naghizadeh & Liu, *supra* note 2, at 2 (discussing how cyber insurance can often lead weaker network security); Pal et al., *supra* note 2, at 9 (noting that, although an insurer is not guaranteed to make a profit by offering cyber insurance, there is substantial societal benefit to having a cyber insurance market).

[96] *See* Naghizadeh & Liu, *supra* note 2, at 2 ("The literature on cyber-insurance has mainly focused on one of the two market environments of competitive or monopolistic insurers. On one hand, it can be shown that in competitive insurance markets, the introduction of insurance contracts not only fails to improve, but can further worsen network security relative to a no-insurance scenario. . . . On the other hand, it is shown that by engaging in premium discrimination, a monopolistic profit-neutral cyber-insurer can induce socially optimal security investments . . . . although [these solutions] implement the socially optimal solution . . . participation is assumed to be mandatory, e.g., users are enforced through policy mandates to purchase insurance.").

insurance provider or mandatory insurance, models of the insurance industry predict that insurers will limit the policies that they offer to first-party contracts that only insure firms against their direct losses in the event of a cyber-incident.[97] Indeed, the literature predicts that such policies can worsen the overall cybersecurity ecosystem by reducing firms' incentives to take precautions to avoid third-party harms that could result from compromise of their systems.[98]

The cyber-insurance market has, in fact, proceeded along these lines. Insurers are generally willing to underwrite first-party policies that protect firms against the direct costs that they incur from a security incident—costs that include investigating and recovering from a cyber-incident, and business losses associated with that incident.[99] And, for that matter, insurers are also happy to underwrite third-party risks.[100]

Although insurers are increasingly underwriting these policies, their breadth of coverage remains substantially unclear. Many of the terms, both in Commercial General Liability (CGL) policies that offer cyber-incident coverage and standalone cyber-insurance policies, remain untested in court.[101] Tellingly, "the ratio of premiums to the coverage limit for cyber insurance is triple the ratio of other liability policies and six times higher than the ratio for property insurance"[102]—a circumstance that both speaks to the uncertainty in the scope of these policies' coverage and that likely makes these policies unattractive to many potential insureds.

What is more, and unsurprisingly, insurers are pushing against broad interpretation of their policies' coverage—or, conversely, for broad construction of these policies' exclusions—at every turn.[103] This is, of

---

[97] *See id.* at 3 (discussing how the optimal insurance contract, for insurers, consists only of a premium and a coverage level).

[98] *Id.* at 2 ("[T]he introduction of insurance contracts not only fails to improve, but can further worsen network security relative to a no-insurance scenario.").

[99] Podolak, *supra* note 2, at 374.

[100] For a comprehensive treatment of both first- and third-party cyber insurance underwriting, *see* Romanosky, et al, *Content Analysis of Cyber Insurance Policies: How do Carriers Develop Policies and Price Cyber Risk?* (draft on file with author).

[101] See, e.g., Lorraine Armenti and Steven Cantarutti, *The Evolution of Cyber Coverage Law: A Survey of Critical Decisions and the Market's Response,* ABA Litigation Committee (Nov 21, 2016) (available at http://www.americanbar.org/publications/litigation-committees/insurance-coverage/articles/2016/fall2016-cyber-coverage.html []); Jeff Sistrunk, *The State of Cyber Coverage Law: 4 Key Decisions*, LAW360 (April 9, 2016 8:53 PM), https://www.law360.com/articles/786246/the-state-of-cyber-coverage-law-4-key-decisions (discussing several recent cases); Kesan, *supra* note 2 (conducting a broad empirical study of cyber insurance litigation, showing that the number of cases filed have tripled in the past 5 years).

[102] Kesan, *supra* note 2, at n. 241.

[103] *See, e.g.*, Lorraine Armenti and Steven Cantarutti, *The Evolution of Cyber Coverage Law: A Survey of Critical Decisions and the Market's Response,* ABA LITIGATION COMMITTEE (Nov 21, 2016), http://www.americanbar.org/publications/litigation-committees/insurance-coverage/articles/2016/fall2016-cyber-coverage.html []; Andrew G. Simpson, *Fallout from Travelers*

course, to be expected. But given the multiplicity of actors in the cybersecurity ecosystem, insurers' efforts to cabin the breadth of their policies limits the regulatory effect of their policies.

Another reason that these policies are often limited is that there is dramatic uncertainty as to the actual risk exposure associated with cyber-incidents. In the context of data breaches, for instance, estimates for the per-record cost of a data breach range from several dollars per record breached to several hundred dollars per record breached.[104] Such a potential range of liability makes it difficult for insurers to construct useful actuarial tables—and therefore limits the range of risks that insurers are willing to underwrite.

This is further compounded by the uncertain legal liability faced as a result of a cyber-incident. As discussed in Section II.B, legal institutions have struggled to adapt to the cybersecurity context. Courts routinely dismiss cases for lack of standing or articulable harm, and where losses are clear the economic loss doctrine often limits recovery.[105] These issues are compounded by adding in insurance contracts, where the terms of these contracts need to be interpreted and given meaning in a new setting—a task with which courts have struggled in recent years.[106] The law, however, continues to evolve, and it is entirely possible that, in any given case, a court may break from the short-lived history of cases in this area and find—potentially substantial—liability. This, again, limits the accuracy of insurers' actuarial tables, and therefore the policies that insurers are willing to underwrite.

A final limitation on the cybersecurity risks that insurers are willing to underwrite is that many risks relating to cybersecurity are correlated. This means that that if one insured is likely to experience a loss, other insureds are similarly likely. This results from the interconnected nature of the Internet and the nature of many cyber-incidents. Any given security vulnerability is likely to affect a large number of insured and exploitation of these vulnerabilities often targets many potential targets simultaneously. A contemporary example is ransomware, which is generally distributed widely by e-mail. A year ago, insurers may not have experienced any ransomware related losses, but today those losses may be widespread across a large

---

CGL Cyber Ruling: Insurance Buyers and Sellers Beware, INSURANCE J. (Apr. 25, 2016), http://www.insurancejournal.com/news/national/2016/04/25/406262.htm []; Sistrunk, *supra* note 101.

[104] *See* PAUL HERSHBERGER, DATA BREACH IMPACT ESTIMATION 3, 10–11, 13 (2016), https://www.sans.org/reading-room/whitepapers/dlp/data-breach-impact-estimation-37502 (discussing the overall cost of data breaches to various organizations and estimating the cost per record breached).

[105] *See, e.g.*, Christopher Scott D'Angelo, *The Economic Loss Doctrine: Saving Contract Warranty Law From Drowning in a Sea of Torts*, 26 U. TOL. L. REV. 591, 591 (1994) (discussing how the economic loss doctrine limits recovery in instances where there is no physical injury to the plaintiff); Opderbeck, *supra* note 35 (discussing various challenges that face cybersecurity related litigation, focusing on the economic loss doctrine).

[106] *See* supra, note 98.

number of insureds.[107] A fundamental principle of risk pooling is that risks cannot be correlated—the fact that one party experiences a loss cannot suggest that others are more likely to experience the same loss. Because many cybersecurity risks are correlated, insurers are, once again, cautious to write broad policies.

V. AN INTEGRATED SOLUTION: CYBERENSURING SECURITY

Sections III and IV discussed the use of strict liability and insurance to address cybersecurity problems. Each has both important positive attributes but also substantial shortcomings. Section V turns to putting these concepts together. Strict liability and insurance have long been recognized to be related concepts—so much so that strict liability is often viewed as a form of insurance.

This discussion begins with an overview of the relationship between strict liability and insurance. This relationship yields a specific policy proposal. Strict liability and cyber insurance are complementary approaches improving the cybersecurity ecosystem. This complementarity can be leveraged by using a strict-liability regime for cybersecurity incidents to promote the development of a more robust cyber insurance marketplace. The "glue" that ties these two mechanisms together is a nuanced damages regime: defendants under the strict-liability regime would face blunt, unforgiving, statutory damages, unless they had an effective cyber-insurance policy, in which case their damages would be limited to the lesser of those statutory damages or actual, provable, damages. The last portion of this Section evaluates this mechanism against the concerns discussed in Sections III and IV.

A. *Strict Liability as Insurance*

The intuitive understanding of strict liability is that it is meant to place the burden of avoiding harm on the more sophisticated party in a relationship—generally the party with greater knowledge about the risks associated with the use of a given product or service. The traditional example is of a dangerous product such as a power tool, which may have some latent defect or require non-obvious training in order to be used safely. Ordinary consumers reasonably need to use such products, but are frequently ill equipped to do so safely. Strict liability seemingly places the burden of ensuring the safety of such products on the manufacturer—the sophisticated party—to ensure that the manufacturer goes beyond the requirements of

---

[107] Lee Matthews, *2016 Saw An Insane Rise In The Number Of Ransomware Attacks*, FORBES (Feb. 7, 2017, 10:36 AM), https://www.forbes.com/sites/leemathews/2017/02/07/2016-saw-an-insane-rise-in-the-number-of-ransomware-attacks/#2b67e3c58dc1 (noting that, while ransomware attacks only rose around 19 percent from 2014 to 2015, the number of such attacks rose by 167% between 2015 and 2016—from roughly 3.8 million to a reported 638 million).

ordinary negligence to also ensure that the product is safe for consumers who may themselves be negligent. This seemingly reasonable understanding is explained on the grounds that the sophisticated party is in a better position to mitigate such harm than its counterparties, so the burden should be placed on the sophisticated party. As Justice Traynor, the author of the *Greenman* opinion commonly heralded as establishing modern strict liability, wrote in an earlier (concurring) opinion, the one in which he first articulated his concept of strict liability: "[P]ublic policy demands that responsibility be fixed wherever it will most effectively reduce the hazards to life and health inherent in defective products that reach the market."[108]

But this is not, in fact, how strict liability operates. Following early adoption of modern forms of strict liability, legal scholars realized—both through theoretical and empirical research—that strict liability does not induce firms (or other parties subject to strict liability) to take greater care to avoid harm than ordinary negligence.[109] The reason for this is simple: ordinary negligence encourages firms to take precautions commensurate with the expected likelihood and magnitude of harm. In other words, under ordinary negligence, firms will invest up to $50 to avoid a 1-in-10 likelihood a $500 harm (that is, an expected $50 in harm). Counterintuitively, however, the transition to strict liability does not change this: a firm will not invest $60 to prevent an expected $50 in harm. Rather, it makes more economic sense for a firm to invest $50 in precaution, hope that the harm does not come to pass, and, if it does come to pass, write a check to the harmed party.

Strict liability, in other words, does not increase either party's incentives to take precautions against harm. Indeed, unless it is implemented with a contributory-negligence defense, it can *encourage* negligent behavior on the part of the non-liable party, since that party knows it is effectively insured against harm by the strictly liable party.[110] Rather than affect parties' incentives, strict liability's real effect is to shift risk of harm from one party

---

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

[109] *See* Epstein, *supra* note 3, at 653 (discussing the moral hazard posed by the proliferation of insurance, namely that insurance often encourages a person to engage in riskier behavior); Priest, *supra* note 3, at 1582–87 (discussing how the increase in tort liability did not lead to an increase in care taken, it only lead to firms losing their insurance due to high premiums and removing their products from the market); Shavell, *supra* note 3, at 124–26 (discussing how strict liability and negligence impact tortfeasor's actions).

[110] See John Prather Brown, *Toward an Economic Theory of Liability*, 2 J. Legal Stud. 323 (1973); Richard Epstein, *The Temporal Dimension in Tort Law*, 53 U. CHI. L. REV. 1175,1178 n.8 (discussing *Toward an Economic Theory of Liability*, explaining that "[w]ith strict liability, however, a defense of contributory negligence matters very much. Under strict liability without defenses . . . some defense of contributory negligence . . . is necessary to prevent the plaintiff from taking unnecessary risks at the defendant's expense."); *see also* William Powers, Jr., *A Modest Proposal to Abandon Strict Products Liability*, 1991 ILL. L. REV. 639, 644 n.18 ("Theoretically, negligence coupled with the defense of contributory negligence provides incentives that tend to optimize safety, while strict liability without contributory negligence does not.").

to another.

The practical consequence of shifting risk in this way is that strictly liable parties become insurers for their counterparties.[111] This is most easily seen in the case of strict products liability. In the first instance, firms will invest in precautions—such as designing their products to minimize the risk of harm through ordinary use—up to that point where the investment in precautions equals the expected likelihood and magnitude of harm. Beyond investing in cost-effective precautions against foreseeable harms, firms will also set aside a portion of their revenues to cover the cost of foreseeable harms that cannot be cost-effectively mitigated. Thus, a firm will invest $50 in precaution to avoid a 1-in-10 chance of a $500 harm (or, more precisely, to minimize the expected likelihood and magnitude of harm as a function of the incremental cost of investment in precautions), but it will also set aside $50 for each unit that it sells in order to compensate the one in ten consumers whom harm is expected to befall. Critically, that $50 set aside for each unit sold does not come from the manufacturer. Instead, the manufacturer passes those costs along to the consumer, increasing the price of its products in order to meet the strict-liability regime's demand that it insure consumers against harm.

In the products-liability market, this is exactly how strict liability works: firms purchase third-party insurance for the users of their products and incorporate the cost of this insurance into their products' prices.[112]

In effect, adopting a strict-liability regime is equivalent to adopting a mandate that parties have insurance against harms that may befall others with whom they interact. That is, strict liability is effectively a mandate for third-party cyber insurance—precisely the sort of insurance that is most likely to yield improvements to the cybersecurity ecosystem, but also precisely the sort of insurance that insurers have been most reluctant to underwrite.

Such a mandate makes sense in many contexts. In the products liability context, for instance, manufacturers have much greater ability to inspect their products and detect latent defects, or to provide basic instruction on the safe use of their products. Even more important, however, they are in a better position to understand the risks of using their products and provide (or purchase) insurance against those risks. It would be very costly to expect the relatively large number of consumers in the economy to research and purchase separate insurance policies for each product they happen to buy—

---

[111] *See* Epstein, *supra* note 3, at 646 (discussing how manufacturers are better able to bear the costs of unforeseen injury and thus are able to act as insurers for their counterparties); Priest, *supra* note 3, at 1525 (theorizing that the purpose behind the expansion of tort liability was as a means to provide insurance to those who could not afford insurance policies); Shavell, *supra* note 3, at 121, 124–26 (noting that under strict liability victims are freed from any risk and essentially insured by their injurers).

[112] *See* Priest, *supra* note 3, at 1559 (noting that consumers suffer when insurance premiums go up because corporations merely increase the costs of their products to compensate).

indeed, in most cases more costly than the value of the product to the consumer. On the other hand, it is relatively inexpensive to require a relatively small number manufacturers to purchase third-party policies. And, on the insurer side, it is relatively costly to negotiate individual policies for individual consumers, each of whom has highly individualized characteristics—but it is relatively inexpensive to negotiate a third-party policy for a large pool of consumers.

The same analysis holds in the cybersecurity context. As was discussed in Section I.D, the difficulties of assigning and quantifying risk under the negligence regime has allowed relatively sophisticated parties to systematically externalize risk onto relatively unsophisticated parties. Under today's model, sophisticated parties underinvest in security and impose the cost of security risks on to unsophisticated parties. And as seen in Section IV, this same pattern has followed into cyber-insurance markets.

This brings us to the key difference between traditional third-party insurance policies and strict liability as insurance: under a traditional insurance policy, coverage is defined and limited by the insurance contract; under a strict liability model, however, coverage is defined by a court's willingness and ability to award damages. Thus, third-party insurance policies may typically cover things such as medical expenses, but are likely to exclude or cap more speculative economic and other non-economic losses. Courts, on the other hand, are more likely and able to award broad economic and non-economic damages.

In the products liability context, in the 1980s this difference proved disastrous.[113] But in the cybersecurity context, this overbreadth of coverage may prove to be a redeeming virtue. The most basic challenges of cybersecurity stem from the multiplicity of actors in the ecosystem, the ease with which they can externalize risk between one another, and the high transaction costs (and difficult litigation environment) that faces anyone seeking to recover damages from malfeasant parties in such an environment. Insurers, it turns out, are uniquely well situated to undertake such an effort—but are only likely to do so if the various risks externalized upon the ecosystem are internalized upon them in a way that they cannot be avoided through contractual exclusion.

B. *Cyberensuring Security: A Unified Model of Strict Cyberliability and Cyber-insurance*

1. *Strict Liability as a Complement to Cyber-insurance*

Sections III and IV of this Article considered the use of strict liability

[113] *See generally* Priest, *supra* note 3 (arguing that adoption of strict products liability since the 1960s drove third-party insurance premiums to unaffordable levels because insurers were forced to cover losses ordinarily excluded from insurance coverage, consequentially rendering insurance unavailable to many).

and cyber insurance, respectively, to improve the overall quality of the cybersecurity ecosystem. There are reasons to believe that each would be an improvement over the status quo—a status quo in which the parties in the best positions to improve cybersecurity face few incentives to do so and in which those parties that do face incentives to improve cybersecurity have little ability to do so. A strict-liability regime could reduce or eliminate the myriad obstacles to bringing a successful suit in response to a security incident; obstacles such as establishing standing, causation, and overcoming the economic loss doctrine.[114] Additionally, an insurance regime inserts a layer of parties into the ecosystem—the insurers—that have an interest in systematically studying and quantifying risks, disseminating knowledge about avoiding them, and pushing for changes that reduce these risks altogether.

We also saw that there are obstacles to adopting either approach. Strict liability would likely need to be implemented by statute, and a strict-liability regime does nothing to resolve the difficulties of determining damages for cybersecurity related harms. And insurers, both facing uncertain legal liability for harms that may befall their insureds and also facing the same uncertainty of indeterminate damages, tend to write narrow policies that do little to address the risks of the broader ecosystem.

The recognition that strict liability is a form of third-party insurance suggests that these approaches may be used jointly, in a way that reinforces the positive attributes of each while helping to overcome their respective limitations. As a form of insurance, strict liability is inherently outward looking, it requires firms to insure others against risks that may occur on the firm's own network or in its software. This would drive demand for broad third-party cyber-insurance policies, which in turn creates the incentive for insurers to work to reduce the risks that inhere in the cybersecurity ecosystem. What is more, treating these harms under a strict liability rule reduces the uncertainty that insurers face, making it easier for them to underwrite policies. These same effects hold even for firms that choose not to purchase a cyber-insurance policy; such firms are merely electing to self-insure against these same harms.

2. *How We Get There: A Policy Proposal*

Unfortunately, there is no way around the fact that a strict-liability regime can only realistically be implemented on a statutory basis. Policy proposals that are contingent upon legislative action—as this one is—are rightly subject to criticism; they are implicitly infeasible and are unlikely to be implemented except in exceptional circumstances. The cybersecurity challenge is such a circumstance. And an effective statutory liability rule

[114] As discussed in Section III, while these "obstacles" serve important functions, in the context of cybersecurity, the complexity of the ecosystem and the nature of harms makes it difficult to successfully litigate even the most meritorious cases.

that would have very dramatic effect can be implemented narrowly.

The essential element of such a statute is that any individual or firm holding records or information about third parties be liable to those parties in the event of a data breach. Data breaches are only one of the many types of potential security incidents that occur on a regular basis. They are, however, a "perfect storm" of the problems facing the cybersecurity ecosystem. Almost every firm today holds consumer information in electronic form, but few of these firms have sophisticated cybersecurity expertise. Rather, they are beholden to the poor incentives of others in the ecosystem to develop and provide them with secure and usable systems. At the same time, they are in the best position relative to their customers to protect their systems and the data stored on them. And, given the indirect relationships between these various parties and the uncertain harms of data disclosure, the prospect of successful litigation under existing legal standards is low. As described in Section III.C, this is a prototypical setting for the use of strict liability.

3. *Cyber-insurance as a complement to strict liability*

Merely implementing a statutory strict-liability rule leaves unresolved the question of damages. As we have seen, the appropriate measure of damages is one of the most substantial challenges facing any liability regime.[115] The simplest way of addressing this is to impose statutory damages alongside the statutory strict-liability regime. But any statutory measure of damages is unlikely to be anywhere near correct. Indeed, inevitably incorrect statutory damages would generally be sufficient reason alone to reject most statute-based policy proposals.

Here, the relationship between strict liability and insurance provides an alternative approach. A key reason that it is difficult to determine an accurate measure of damages is that there is a lack of actual data about the consumer costs of data breaches. Insurance companies are in the business of collecting, analyzing, and using just this sort of data—this is, in a very real way, the heart of the insurance business. This expertise can be leveraged here.

Rather than impose statutory damages, a statutory strict-liability rule should be accompanied by presumptive but rebuttable statutory damages. Under this model, an appropriate agency—such as the FTC, which has substantial experience investigating data breaches—would be tasked with developing a schedule of presumptive damages for different sorts of data that can be compromised in data breaches.[116] In constructing this schedule, the agency would be instructed to err on the side of finding liability for

---

[115] *See supra* notes 37–40 and accompanying text (discussing how courts have struggled to understand the damages associated with security incidents); *see also* HERSHBERGER, *supra* note 1044 (discussing the range of losses attributable to a data breach on a per-record basis).

[116] As part of this statute, the FTC would also be statutorily barred from taking administrative enforcement actions against firms that experience data breaches.

damages even in the absence of substantial evidence supporting such damages, but not in the face of countervailing substantial evidence that damages are in fact less. Any firm that experiences a breach would be subject to these damages *unless* it had a cyber-insurance policy that covered the third-party harms, in which case damages would be assessed as actual provable damages, with the statutory damages as a backstop in the event that there was insufficient evidence to establish actual damages.

C. *Evaluating Cyberensured Security*

The policy proposed above is designed to take advantage of—indeed, to "supercharge"—the relationship between strict liability and insurance. The imposition of strict liability for certain cybersecurity incidents effectively imposes a third-party liability insurance requirement on firms holding consumer data. This requirement, in turn, would create a substantial demand for comprehensive third-party liability insurance policies. As insurers enter this market, the presumptive statutory damages would create an incentive for insurers to collect and put to use data on actual damages—providing much needed information that is currently lacking in current cybersecurity research. And insurers would also have their traditional incentives to improve their insureds' practices and the overall quality of the security ecosystem in order to reduce their exposure to risk. No one else today is in a position to undertake these efforts on a systematic basis.

This policy does have important limitations and possible challenges. Most important, by design this would only impose liability on consumer-facing entities that host consumer data. This is in part paean to practicality. A greater scope of liability would make it more difficult for an idea such as this to actually be implemented. And this also focuses attention on the part of the cybersecurity ecosystem where attention both is arguably most needed and will be most effective.

This is not to say that this policy would not have effects throughout the broader ecosystem. As an initial matter, the relationship between the multiplicity of actors that make up the ecosystem would continue to be governed by contract. Today, these contracts generally broadly disclaim liability for security-related incidents. This is in part a reflection of the general lack of liability in the ecosystem—sophisticated firms, knowing that they are unlikely to face significant liability should they experience a breach, are unconcerned about contractually waiving liability claims, and less sophisticated firms are generally not in a position to negotiate alternative terms. This dynamic would likely change, however, under an insurance model; insurers would both understand, and be in a position to insist upon, more favorable terms to protect their insureds (and themselves). What is more, the insurers are in a position to litigate these terms.

A final concern that must be acknowledged about this approach is that it could expose firms to a literally overwhelming amount of risk—enough

risk that insurers would refuse to underwrite it and that firms subject to liability would go out of business. This is, in fact, what happened in many industries subject to strict liability rules in the 1980s.[117] If a contemporary manifestation of the insurance crisis of the 1980s does occur, it is unquestionably the case that a change in policy would be necessary. In and of itself, however, this occurrence would be important data for how we should develop new policy. If the scope of cyber-insecurity and related data losses is so great that these losses are uninsurable, that raises fundamental questions about the nature of the Internet economy.

In this way, a policy such as this focuses attention directly upon what is the uncertain, and uncomfortable, question at the core of the modern economy: how sensitive and valuable are the trillions of bits of information about billions of people hosted on millions of insecure computers around the world? In the eyes of many, this information is incredibly valuable, and the potential harms that individuals face from its misuse or appropriation are substantial; to others, this information has nearly zero value, and whatever harms its misuse or compromise yield are anyhow ephemeral, intangible, and insufficiently concrete to justify any damages. Under the former view, we are woefully underinvesting in security—or, more likely, the entire edifice of the Internet is a ticking time bomb of impending, and uninsurable, cyber-liability. In either event, pushing the market to internalize whatever liability exists through express liability and insurance mechanisms can only serve to improve upon the status quo.

CONCLUSION

Cybersecurity is among the most challenging, most important, issues of the day. Cyber insurance and strict liability for certain types of cyber incidents are among the approaches frequently discussed to address the challenge of cybersecurity. Neither approach on its own, however, has yet managed to achieve its potential. Imposing strict liability—a step that no court or regulator has yet taken—for instance, leaves unaddressed complex questions of damages. And left to its own devices, the cyber-insurance market will narrow the policies it underwrites to avoid the most difficult (and most important to address) aspects of the cybersecurity ecosystem.

This Article's key contribution to the issue is the observation that strict liability and cyber insurance are complementary sides of a single coin. It turns out that insurance and strict liability are intimately related, however—and that they are related in ways that allow each to complement and correct the weaknesses in the other. This observation offers helpful insights into ongoing discussions about both strict liability and cyber insurance—insights that are useful to both subject areas independently, as well as important as a

[117] *See* Priest, *supra* note 3, at 1521 (discussing the insurance crisis of the 1980s and its effect on the economy).

way to bring these discussions under a common framework.

Drawing from these insights, this Article has proposed a strict-liability rule for harms deriving from cyber-incidents. Under this rule, consumer-facing firms that use or store consumer information would be strictly liable to those consumers for any security incidents (i.e., data breaches) involving that data. In order to work, this rule would impose administratively defined statutory damages, but firms that have cyber insurance policies covering third-party harms would only pay the lesser of those statutory damages or actual provable damages for insured claims.

The characteristics of this model compare favorably to the current status quo—one wherein users are largely helpless, firms are largely unknowledgeable, software is generally insecure, federal agencies are generally impotent to bring about meaningful change in the structure and operation of private markets, and attackers are largely judgement-proof.