INSURING EVOLVING TECHNOLOGY

ASAF LUBIN*

ABSTRACT

The study of the interaction between law and technology is more critical today than ever before. Advancements in artificial intelligence, information communications, biological and chemical engineering, and space-faring technologies, to name but a few examples, are forcing us to reexamine our traditional understanding of basic concepts in torts and insurance law.

Yet, few insurance professionals and scholars will identify themselves as working in the field of "law-and-technology." For many of them, technology is "just a fact about the world like any other," as Ryan Calo once put it, not one that always merits "special care."[1]

This short paper is an attempt to build a first-of-its-kind bridge between these two scholarly silos. Directed at an insurance audience, the paper attempts to draw attention to a body of law-and-technology scholarship that has so far gone mostly unnoticed by insurance professionals.

The paper is built on the premise that insurance lawyers, whose business model depends on the mitigation of losses from technological harm, are not dramatically dissimilar from their law-and-technology counterparts. Both are fascinated by the same set of questions: if, when, and how, might

---

* Dr. Asaf Lubin is an Associate Professor of Law at Indiana University Maurer School of Law, a Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard University, a Visiting Fellow at the Information Society Project of Yale Law School, a Visiting Scholar at the Federmann Cybersecurity Center at Hebrew University of Jerusalem, a Fellow at the Center for Applied Cybersecurity Research at Indiana University, and a Visiting Fellow at the Nebraska Governance and Technology Center at the University of Nebraska. I wish to thank Dan Schwarcz, Gus Hurwitz, Demet Batur, Matthew Schaefer, Tammi Etheridge, and João Marinotti for terrific feedback on earlier drafts of this paper. I further wish to thank all the participants of the "Cyber Cyber Insurance Law Conference" organized jointly by University of Connecticut Insurance Law Center and the University of Minnesota Law School, as well as participants in the Nebraska Governance and Technology Center Fellows' Workshop and the Henry Jackson Society Cyber Insurance event. Finally, I wish to thank the editors of the Connecticut Insurance Law Journal for their consideration of this piece.

[1] Ryan Calo, *Commuting to Mars: A Response to Professors Abraham and Rabin*, 105 VA. L. REV. 84, 88 (2019).

private and public regulation mitigate losses resulting from technological risk. The paper draws key concepts from the law-and-technology literature to explore the effectiveness and utility of regulation in mitigating risks from emerging, evolving, and disruptive technologies. The paper further identifies the different phases in technology's life cycle and discusses the challenges that each of these phases introduces on the insurance market.

Relying on cyber insurance as its primary case study, the paper concludes by applying these insights to an assessment of a recent state-wide regulation, the New York Cyber Insurance Risk Framework, the first of its kind in the country. The paper demonstrates the promise and pitfalls of this type of regulation, taking into account broader trends in the cyber insurance market.

TABLE OF CONTENTS

INTRODUCTION

On March 12, 2021, the University of Minnesota and the University of Connecticut Insurance Law Center co-organized *A Cyber Cyber Insurance Conference* to examine the current state of our evolving cyber

insurance markets.[2] The organizers wisely devoted one of the panels to the unique position of government in fostering these markets.[3] As the event's website further noted, panelists were called to "explore what state and federal governments can, and should, do to promote more robust cyber insurance markets."[4]

As I was contemplating my written contribution for this symposium, I was struck by just how much has been written over the years on this very topic. Academics, international organizations, and cyber insurance specialists have produced mountains of lengthy and persuasive accounts of possible areas for regulatory reform.[5] Jay Kesan and Carol Hayes, for

---

[2] For more information about the conference, see *The Role of Law and Government in Cyber Insurance Markets: A Cyber Cyber Insurance Conference*, UNIV. OF CONN. SCH. OF L.: INS. L. CTR., https://events.uconn.edu/event/78763/2021-03-12 (last visited Jan. 31, 2022).

[3] *Id.*

[4] *The Role of Law and Government in Cyber Insurance Markets: A Cyber Cyber Insurance Conference,* EVENTBRITE, https://www.eventbrite.com/e/the-role-of-law-and-government-in-cyber-insurance-markets-registration-133229401727 (last visited Jan. 31, 2022) (reservation website).

[5] *See, e.g.*, OECD, ENHANCING THE ROLE OF INSURANCE IN CYBER RISK MANAGEMENT 135–37 (2017) [hereinafter OECD REPORT] ("Governments could contribute to the availability of data on past cyber incidents, forward-looking analyses on the changing nature of the risk and on the effectiveness of security practices, including through the development or promotion of cyber security standards. Governments should also closely monitor the market developments and consider if there is a need to intervene to encourage greater clarity on coverage or to support the management of accumulation risk."); EUR. INS. & OCCUPATIONAL PENSIONS AUTH., UNDERSTANDING CYBER INSURANCE – A STRUCTURED DIALOGUE WITH INSURANCE COMPANIES 25 (2018) (exploring the following potential contributions of regulations: (1) regulation of appropriate pricing and monitoring of the risks, including potential aggregation risks; (2) promotion of incident reporting and exchange of information; (3) enhancing a better understanding of risks; (4) introduction of minimum IT and Information security standards; (5) increase the level of awareness and prudence of new entrants (both insurers and buyers); (6) ensure adequate capital requirements against underwriting risks; (7) prevention of contagion in case of bigger scale); Justin (Gus) Hurwitz, *Cyberensuring Security*, 49 CONN. L. REV. 1495, 1499–500 (2017) (proposing "a strict-liability rule for harms deriving from cyber-incidents" noting further that "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."); Minhquang N. Trang, Note, *Compulsory Corporate Cyber-Liability Insurance: Outsourcing Data Privacy*

example, have discussed the prospect of "government subsidies for both insurance and security technology."[6] Michael Faure and Bernold Nieuwesteeg highlighted the role that government regulation of cybersecurity practices could play in setting normative cues for cyber insurance, particularly in the context of cyber risk pools.[7] Jan Lemnitzer called on governments to: develop minimum cybersecurity standards for small-to-medium businesses ("SMEs"), set up a claims database to increase data sharing, and announce the intention to make cyber insurance compulsory for SMEs in the near future.[8] Kenneth Abraham and Daniel Schwarcz have explored the prospect of a federal reinsurance program for cyber catastrophes.[9] Daniel Woods and Andrew Simpson have gone even further by mapping out no less than twenty-three different possible government interventions, breaking them down into six general themes, which were then introduced as part of an overarching framework and research roadmap for future scholarship.[10]

Regulation to Prevent and Mitigate Data Breaches, 18 MINN. J.L. SCI. & TECH. 389 (2017) (calling for a mandatory cyber risk regime); Brendan Heath, Note, *Before the Breach: The Role of Cyber Insurance in Incentivizing Data Security*, 86 GEO. WASH. L. REV. 1115, 1137–39 (2018) (discussing governmental regulatory options around standard setting and information dissemination); Nehal Patel, Note, *Cyber And TRIA: Expanding the Definition of An "Act of Terrorism" to Include Cyber Attacks*, 19 DUKE L. & TECH. REV. 23 (2021) (proposing amendments to the Terrorism Risk Insurance Act so that the Act more clearly covers acts of cyberterrorism); Kyle D. Logue & Adam B. Shniderman, *The Case for Banning (and Mandating) Ransomware Insurance*, 28 CONN. INS. L.J. (forthcoming 2021) (manuscript 1) (proposing a "limited ban on indemnity for ransomware payments with exceptions for cases involving threats to life and limb, coupled with a mandate that property/casualty insurers provide coverage for the other costs of ransomware attacks.").

[6] Jay P. Kesan & Carol M. Hayes, *Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment*, 102 MINN. L. REV. 191, 273–76 (2017).

[7] Michael Faure & Bernold Nieuwesteeg, *The Law and Economics of Cyber Risk Pooling*, 14 N.Y.U. J.L. & BUS. 923, 959 (2018).

[8] Jan Martin Lemnitzer, *Why Cybersecurity Insurance Should be Regulated and Compulsory*, 6 J. CYBER POL'Y 118, 125–26, 128–31 (2021).

[9] Kenneth S. Abraham & Daniel Schwarcz, *Courting Disaster: The Underappreciated Risk of Cyber Insurance Catastrophe*, 27 CONN. INS. L.J. 1, 64–66 (2021).

[10] Daniel Woods & Andrew Simpson, *Policy Measures and Cyber Insurance: A Framework*, 2 J. CYBER POL'Y 209, 221 tbl.2 (2017).

Admittingly, I also contributed to this growing heap of cyber insurance regulation scholarship. In my latest work, I relied on public policy arguments to make the case for a set of governmental interventions in the markets, particularly around the indemnification of: "(1) acts of cyber terrorism or state-sponsored cyber operations; (2) extortion payments for ransomware attacks; and (3) administrative fines for violations of statutory data protection regulations."[11]

It is important to note that all of these proposals have yet to be implemented in any meaningful way, including in North America,[12] the largest cyber insurance market in the world.[13] While some changes have certainly occurred around the margins,[14] for the most part, the status quo on

---

[11] Asaf Lubin, *Public Policy and the Insurability of Cyber Risk*, 5 J.L. & TECH. TEX. (forthcoming 2022) (manuscript at 1–2).

[12] The National Defense Authorization Act for Fiscal Year 2021 includes a provision for Government Accountability Office (GAO) to study the U.S. cyber insurance market. H.R. 6395, 116th Cong. 33 (2020) (enacted). In May 2021 GAO produced a report summarizing many of these proposals and submitted them to the appropriate congressional committees and the Secretary of the Treasury for consideration. To date, it does not appear that any substantive measures have been taken to implement the report's proposals. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-477, CYBER INSURANCE: INSURERS AND POLICYHOLDERS FACE CHALLENGES IN AN EVOLVING MARKET (2021).

[13] *World Cyber Insurance Market to Reach $14 Billion by 2022: Report*, BUS. INS. (Dec. 7, 2016), https://www.businessinsurance.com/article/20161207/STORY/912310861/World-cyber-insurance-market-to-reach-$14-billion-by-2022-Report ("A report by U.S.-based market research firm Allied Market Research has said that the global cyber insurance market is expected to grow at a compounded annual growth rate of 28% between 2016 and 2022 to reach $14 billion by 2022 . . . . North America is expected to hold the largest cyber insurance market share during the forecast period, driven by enforcement of data protection regulations in the United States, increases in levels of liability and legislative developments.").

[14] On the issue ransomware, the U.S. Treasury Department issued an advisory at the end of 2020, which warns companies not to pay ransom to sanctioned entities. *See* U.S. DEP'T OF TREASURY, ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS (2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf. In September 2021 the Department issued an updated advisory that noted that the Office of Foreign Asset Control (OFAC) when evaluating possible enforcement outcomes will consider "full and ongoing cooperation with law enforcement both during and after a ransomware attack — e.g., providing all relevant information such as technical details, ransom payment demand, and ransom payment instructions as soon as possible — to be a significant mitigating factor." U.S. DEP'T OF TREASURY, UPDATED ADVISORY ON

cyber insurance remains. Why have legislatures and regulators been so slow to adopt any of these proposals? Perhaps, we have been looking at cyber insurance regulation through the wrong lens.

So far, we have focused much of our collective theorizing on *sui generis* interventions, tailored and designed to the specific risks of cyberspace.[15] But cyber insurance is, after all, merely a sub-category within a broader umbrella of insurance products, which are designated to transfer risks from evolving technologies (from a products liability insurance for 3D

POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS 5 (2021), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf. This includes the company's "self-initiated and complete report of a ransomware attack to law enforcement or other relevant U.S. government agencies . . . ." *Id.* The updated advisory extends to companies involved "in facilitating ransomware payments on behalf of victims" (thereby potentially extending the advisory to insurers and other actors involved in the negotiation with the hackers on behalf of victims). *Id.* at 4. Nonetheless, it should be noted that so far only limited enforcement action has been taken by OFAC against the payment of ransom. *See* Michael T. Borgia & Dsu-Wei Yuen, *OFAC Makes Waves in Fight Against Ransomware, but Practical Effects Unclear*, DAVIES WRIGHT TREMAINE LLP (Oct. 1, 2021), https://www.dwt.com/blogs/financial-services-law-advisor/2021/10/ofac-updated-ransomware-advisory (clarifying that at the end of 2021 OFAC issued its "first-ever sanctioning of a cryptocurrency exchange for transacting with ransomware gangs" but suggesting that "standing alone", such limited OFAC action, while "significant" by themselves, nonetheless generate "unclear" actual effects on deterrence.).

On the issue of developing cybersecurity standards, it should be noted that a few states (namely, Utah, Indiana, and Ohio) have either adopted or are in the process of adopting cybersecurity safe harbor rules. These rules provide covered entities with immunity from liability in state courts for any cybersecurity or data breach, subject that the company commits and complies with certain cybersecurity standards and frameworks laid down in the law. *See generally New Ohio Law Creates Safe Harbor for Certain Breach-Related Claims*, HUNTON ANDREWS KURTH: PRIV. & INFO. SEC. L. BLOG (Nov. 5, 2018), https://www.huntonprivacyblog.com/2018/11/05/new-ohio-law-creates-safe-harbor-certain-breach-related-claims/; Romaine Marshall, *Utah Considers a Cybersecurity Safe Harbor as Ransomware Runs Rio*t, JD SUPRA: GLOB. PRIV. & SEC. BLOG (Feb. 26, 2020), https://www.jdsupra.com/legalnews/utah-considers-a-cybersecurity-safe-96201/; Gretchen M. Rutz, John L. Landolfi, Christopher L. Ingram, Christopher A. LaRocco & Sarah Spector Boudouris, *Indiana Attorney General to Create Safe Harbor for Businesses that Implement Reasonable Cybersecurity Plans*, LEXOLOGY (Sept. 28, 2020), https://www.lexology.com/library/detail.aspx?g=da29facf-7ea3-4439-ba25-28b5479577b6.

[15] *See, e.g.*, Jeffrey L. Vagle, *Cybersecurity and Moral Hazard,* 23 STAN. TECH. L. REV. 71, 85 (2020) (discussing the "*sui generis* principal-agent problem" of cybersecurity).

printed products[16] to automobile insurance for autonomous vehicles[17]). Might we, therefore, be better served, when thinking about the utility of regulating these markets, if we considered the larger network effects at the intersection of torts, insurance law, technological evolution, and social adoption?

It is undisputed that "evolving technologies generate novel questions and that these questions sometimes give rise to thorny cases."[18] What is more fraught, however, is the idea, taken up by law-and-technology scholars, that questions motivated by different technological changes and dynamics nonetheless share some underlying similarities.[19] For the law-and-technology folk, these questions arise for similar reasons and are answered in similar ways, justifying the adoption of a single unified theory.[20] As Lyria Moses argued: "[r]ecognizing the similarities between problems arising in different technological contexts creates the possibility of learning from the consequences of past legal responses to technological change."[21]

Unfortunately, legal analysis is the land of doctrinal segregation and isolationism. "Lawyers tend to break along technological lines (health lawyers, cyber-lawyers, etc.) or doctrinal lines (contract lawyers, tort lawyers, etc.)."[22] While legal specialization is certainly welcome—especially where it aims to improve the quality of legal service and reasoning while reducing the costs of conducting research and analysis[23]—at times it is hindering and even blinding. After all, insurance lawyers whose business model depends on the mitigation of losses from technological harm are not

---

[16] *See, e.g.*, Jordan Lipp & Steven Michalek, *3D Printing: Product Liability, Professional Liability and Other Tort Aspects of the Burgeoning Industry*, DEF. COUNS. J., Apr. 2020, at 1, 6 (2020); TRAVELERS INDEM. CO., HAVE YOUR 3D PRINTED CAKE AND EAT IT TOO 17 (2016), https://www.travelers.com/iw-documents/business-insurance/tech-3D-whitepaper-BTCWH.0003-D.pdf.

[17] Automated and Electric Vehicles Act, 2018, c. 18 (U.K.), https://www.legislation.gov.uk/ukpga/2018/18/contents (the act applies the existing insurance infrastructure and requirements from traditional automobiles to autonomous vehicles).

[18] Mason v. Mach. Zone, Inc., 140 F. Supp. 3d 457, 469 (D. Md. 2015).

[19] *See* Lyria Bennett Moses, *Why Have a Theory of Law and Technological Change?*, 8 MINN. J.L. SCI. & TECH. 589, 594 (2007).

[20] *See id.*

[21] *Id.* at 598.

[22] *Id.* at 594.

[23] *See generally* Clarke B. Rice, Comment, *Legal Specialization: A Proposal for More Accessible and Higher Quality Legal Services*, 40 MONT. L. REV. 287, 288 (1979).

dramatically dissimilar from their law-and-technology counterparts. Both are fascinated by the same set of questions: if, when, and how, might private and public regulation mitigate losses resulting from technological risk?

This short paper is an attempt to build a first-of-its-kind bridge between these two scholarly silos.[24] Directed at an insurance audience, the paper attempts to draw attention to a body of law-and-technology scholarship that has so far gone mostly unnoticed by insurance professionals. The paper is divided into three parts. Part I identifies the different phases in a technology's life cycle and discusses the challenges that each of these phases introduces on the insurance market for risks resulting from technology's continuous evolution. Part II then moves to explore the law-and-technology literature to distill key understandings about the effectiveness and utility of governmental interventions in mitigating risks from emerging, evolving, and disruptive technologies. This section identifies three primary lessons learned, focusing on the intersections between technology and classification, regulation, and globalization. Finally, Part III returns to the cyber insurance debate to apply these lessons. In particular, the section looks to assess the merits of the New York Insurance Regulator's recent Cyber Insurance Risk Framework[25] as the first ever state-wide cyber insurance regulation in the United States. The paper discusses the promise and limits of this regulation in the broader context of the insights from law-and-technology literature and emerging trends in the cyber insurance market.

---

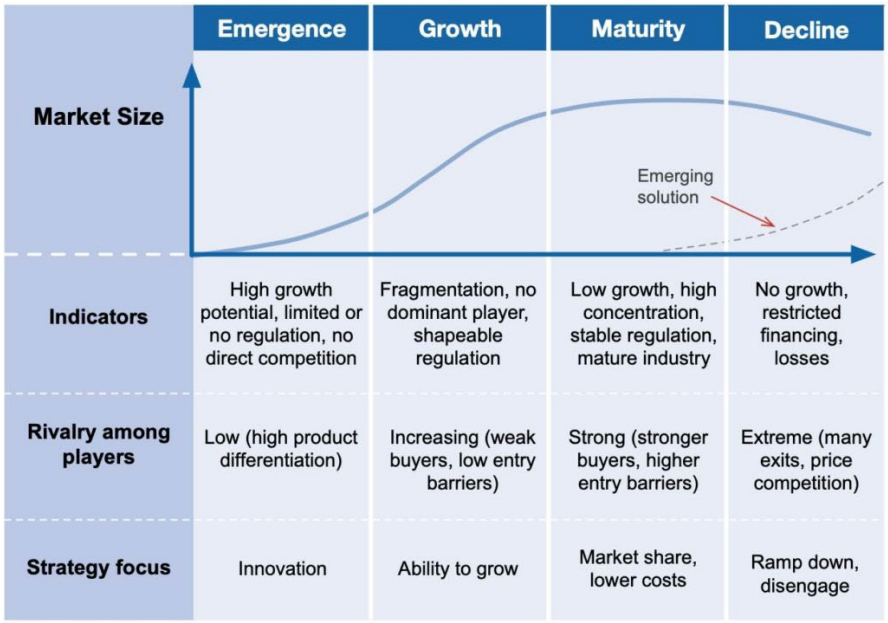
[24] Ryan Calo, responding to a paper by Kenneth Abraham and Robert Rabin on liability and insurance for autonomous vehicles, demonstrated the existence of these scholarly silos. He noted, "[t]he puzzle of how to deal with the contingency of technology and its social impacts is not limited to driverless cars, but endemic to law and technology scholarship. Personally, I doubt Professors Abraham and Rabin—each renowned scholars of civil liability—identify themselves as working in 'law and technology' as such. I imagine that for the authors, the ascendance of automated vehicles is just a fact about the world like any other, as the progress of technology often is. In my experience, however, reasoning about technological change sometimes requires special care." Calo, *supra* note 1, at 87–88 (2019) (footnote omitted).

[25] Letter from Linda A. Lacewell, Superintendent, N.Y. State: Dep't Fin. Servs., to All Authorized Prop./Cas. Insurers (Feb. 4, 2021), https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02.

I. BETWEEN TORTS, INSURANCE, AND TECHNOLOGICAL EVOLUTION

Technological changes are those involving "any tool or technique, any product or process, any physical equipment or method of doing or making, by which human capability is extended."[26] Such extensions can take myriad forms. The invention of the first iPhone is different from the invention of the iPhone 8. While both are technological changes extending human capability, one is emerging and disruptive, while the other offers a minor expansion within an already established line of innovation, causing far limited ripple effects.[27]

Illustration 1: Phases of an Industry Life Cycle[28]



---

[26] DONALD A. SCHON, TECHNOLOGY AND CHANGE 1 (Dell Publ'g Co. 1967)

[27] *See* Peter Huber, *Safety and the Second Best: The Hazards of Public Risk Management in the Courts*, 85 COLUM. L. REV. 277, 298 (1985) ("New products and processes, though never risk-free in themselves, usually prove to be less hazardous than the older, manmade substitutes they replace.").

[28] SUN WU, STRATEGY FOR EXECUTIVES 21 (Strategy for Execs. ed., 2019 ed. 2019).

As technology matures, our understanding of the risks associated with its deployment and use changes.[29] This includes both first-party harms (those harms that first adopters of the technology might incur directly from using such an emerging technology) and third-party harms (the possible liabilities for damages to others from the development and deployment of a new technology).[30] The latter harms are perhaps even more fundamental as the introduction of such liability could significantly stifle creativity and innovation.[31] In thinking about technological risk, its evolution over time, and its interplay with insurance as a mitigating tool, we may wish to rely on a classic industry life-cycle model. At each stage of the model—from the embryotic pre-emergence stage, to the emergence stage, to the growth stage, to the maturity and ultimate decline stages—different kinds of insured risks could be potentially introduced, and those may impact different categories of policyholders along the supply chain in different ways: from developers, to manufacturers, to distributors, to consumers.

Especially at the embryotic and emergent phases, where technology is most unstable, challenges would arise in both torts and insurance around the issue of liability.[32] Indeed, the law often treats developers and first

---

[29] *See The Evolution of Risk in the Face of Technology,* ZURICH (Nov. 10, 2014), https://www.zurich.com/en/knowledge/topics/global-risks/the-evolution-of-risk-in-the-face-of-technology (discussing how evolving technology generates "fresh risks.").

[30] As applied in the context of cyber insurance specifically see Lubin, *supra* note 11, at 6–7.

[31] *See, e.g.*, Fred Roeder, *How Liability Lawsuits Drive Up Drug Prices, Stifle Innovation, and Harm Patients*, CONSUMER CHOICE CTR. (May 7, 2020), https://consumerchoicecenter.org/how-liability-lawsuits-drive-up-drug-prices-stifle-innovation-and-harm-patients/; U.S. CHAMBER INST. FOR LEGAL REFORM, THE FUTURE OF AI LIABILITY IN THE EU: PROTECTING CONSUMERS WITHOUT STIFLING INNOVATION 20 (2020) (discussing how changes to the existing liability regime in AI regulation could stifle innovation).

[32] *See* Dennis R. Connolly, *Insurance: The Liability Messenger, in* PRODUCT LIABILITY AND INNOVATION: MANAGING RISK IN AN UNCERTAIN ENVIRONMENT 131, 135 (Janet R. Hunziker & Trevor O. Jones eds., 1994) ("[T]he more scientifically advanced the product, the more uncertainty it is likely to engender in insurers. Precisely because it is such a departure from other products, it has no track record and thus provides no solid basis for predicting and pricing the risks involved."); Peter W. Huber, *Junk Science in the Courtroom: The Impact on Innovation, in* PRODUCT LIABILITY AND INNOVATION: MANAGING RISK IN AN UNCERTAIN ENVIRONMENT 138, 138 (Janet R. Hunziker & Trevor O. Jones eds., 1994) ("It is the new venture with the unfamiliar product that can least tolerate the

adopters "as taking their chances with a technology," [33] assigning all costs for potential harms from creating and using the technology to them.[34] Courts "greatly prefer natural, old, or established hazards to those deriving from new technologies."[35] As such, their early rulings may set chilling effects on continued development and use of the technology.[36] Insurers, in turn, will either not offer the coverage or offer only limited protections with significantly high premiums.[37]

Government interventions at this stage could focus on creating a counterbalance to these inherent disincentives within the law on innovation, research, and design of new technologies. This is because "[t]here is hardly a product in use today—a car, plane, boiler, municipal water system, drug, vaccine, or hypodermic syringe—that is not many times safer than its counterpart of a generation or even a decade ago."[38] So, to the extent that "[i]nnovation and technological change . . . reduce risk,"[39] the government would benefit from summoning the courage and implementing the incentive structure so that developers and users may survive the turbulent embryotic and emergent period.[40]

---

extra measure of instability from the legal environment that does not provide predictable results.").

[33] Kyle Graham, *Of Frightened Horses and Autonomous Vehicles: Tort Law and Its Assimilation of Innovations*, 52 SANTA CLARA L. REV. 1241, 1260 (2012).

[34] *See* Connolly, *supra* note 32, at 134 (noting the various ways state laws can be "insurer-unfriendly").

[35] Huber, *supra* note 27, at 307.

[36] Graham, *supra* note 33, at 1268–70.

[37] Trevor O. Jones & Janet R. Hunziker, *Overview and Perspectives, in* PRODUCT LIABILITY AND INNOVATION: MANAGING RISK IN AN UNCERTAIN ENVIRONMENT 1, 2 (Janet R. Hunziker & Trevor O. Jones eds., 1994) ("Even though product safety may have been improving, companies were experiencing more product liability cases and the size of the awards was increasing. As a result, their insurance costs were going up and for some products, insurance coverage was being withdrawn altogether.").

[38] Huber, *supra* note 27, at 298.

[39] *Id.* at 298–99.

[40] For an alternative view, one that posits that technology does not evolve in a linear way towards ultimate safety, see Vagle, *supra* note 15, at 92–94 (suggesting that the "uniquely American concept of technology advancement," as adopted by Silicon Valley, is one of "innovation-over-maintenance." According to this approach, companies prefer the ability "to rapidly move from idea to prototype to product" even if that comes at the expense of their customers' security. "One of the more significant problems with this approach is the increased risk associated with a

A more nuanced view suggests that different technologies would experience different embryotic stages, with tort and innovation interacting in different ways. Some technologies will "produce 'too many' lawsuits" while others might produce "too few."[41] This is because legal uncertainty "can cut two ways."[42]

> Uncertainty as to the prospect, viability, and magnitude of tort claims regarding an invention may chill its development and diffusion. But uncertainty as to matters such as the existence of a cause of action and the likelihood of recovery also may stifle the filing of claims that attack the innovation as unreasonably dangerous.[43]

The nature of the technology, the scope and magnitude of its likely harms, and the volume of harmful occurrences that actually materialize, would all play a role in the cost-benefit analysis behind prospective litigation and liability insurance.

In any event, a common theme along the time continuum of the technology life cycle is the notion that "uncertainty does give way to knowledge over time. Society learns as it produces and assembles information about technological hazards."[44] With information comes a better ability to regulate and set expectations of behavior and duties of care; with that the risk becomes "fully assimilated within everyday tort law."[45] Insurers appreciate this level of stability, which translates in turn into lower premiums and higher caps as risk modeling and management solidifies.

But law continues to interact with the technology even after it has fully matured. Danielle Citron carefully described how law, as designed by

---

company's inability (or unwillingness) to seriously consider the negative consequences of their design decisions in the race to innovate.").

[41] *See* Graham, *supra* note 33, at 1269.

[42] *Id.* at 1268.

[43] *Id.* at 1268–69.

[44] Mary L. Lyndon, *Tort Law and Technology*, 12 YALE J. ON REG. 137, 141 (1995).

[45] Graham, *supra* note 33, at 1242. If to use Baker's terminology, once a technology reaches a certain maturity then "tort doctrine and the consistent behavior of insurance adjusters" will begin to converge. Tom Baker, *Liability Insurance as Tort Regulation: Six Ways That Liability Insurance Shapes Tort Law in Action*, 12 CONN. INS. L.J. 1, 12 (2005). This is because "street level bureaucrats" will over time begin to take over "the bulk of the tort law universe" to a point where tort law and insurance practice engage in regular and mutually beneficial conversation. *Id.*

courts, regulators, and legislatures, might interact with technology throughout its life cycle:

> First, it recognizes the new form of harm, but not the benefit that the new technology has occasioned. This drives the law to adapt existing theories of liability to reach that harm. Second, after the technology's benefits become apparent, the law abruptly reverses course, seeing its earlier awards of liability as threats to technological progress and granting sweeping protection to the firms in the new industry. Finally, once the technology becomes better established, the law recognizes that not all liability awards threaten its survival. It then separates activities that are indispensable to the pursuit of the new industry from behavior that causes unnecessary harm to third parties.[46]

External actors, such as reinsurers, might need to step in at different stages to offer an intervention. Think about developments in engineering technologies in the United States in the nineteenth and early twentieth centuries. "[T]he scope of challenging engineering projects—from larger and more complex manufacturing, infrastructure, and aircraft—were now beyond the capacity and expertise of a single insurer. These risks required a new level of expertise and risk management not readily available within the ranks of US insurers."[47] Established European reinsurers, such as Swiss Re, "extended their capacity to reinsure these single, large risks in collaboration with insurers and large corporate clients."[48] Reinsurance thus stepped in to provide a safety net and a necessary degree of assurance for innovation to be tested, proven, and ultimately assimilated.

Where insurance and reinsurance are not available, the government might take a more active role. Consider the United States government indemnification frameworks for commercial space-flight operators. The operators are required to obtain "third-party liability insurance in the amount of the maximum probable loss (MPL), according to a calculation performed

---

[46] Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 115 (2009) (footnotes omitted).

[47] SWISS RE CORP. HIST., A HISTORY OF US INSURANCE 24 (2017), https://www.swissre.com/dam/jcr:36ebe594-097d-4d4d-b3a7-2cbb8d856e85/150Y_Markt_Broschuere_USA_EN_Inhalt.pdf.

[48] *Id.*

by the FAA [Federal Aviation Administration]."[49] Where the third-party liability claims exceed the MPL, "the government has in essence made a statutory promise to pay for the next tier, or tranche, of up to $2.8 billion dollars in any third-party liability claims faced by the space-flight entity."[50] Because the advancement of a vibrant commercial space industry is a matter of national security importance to the United States and its economy, the government is willing to step in and offer this promise.[51]

II. LESSONS LEARNED FROM LAW AND TECHNOLOGY LITERATURE

A complex set of questions goes into an *entity's decision to generate new law* in a technologically evolving environment. These questions include: What do we mean by "*new law"*? Who is the "*entity*" that makes that decision? And what forms might "*law generation*" take? Law-and-technology scholars have been fascinated by these questions. Their ability to answer these questions effectively is rooted in their willingness to approach such questions not solely from a legal or economic perspective. Rather, many of these scholars adopt an interdisciplinary lens that is socio-legal. For them, regulation is not merely the "promulgation of an authoritative set of rules, accompanied by mechanisms . . . for monitoring and promoting compliance with these rules."[52] They step outside of what Christel Koop and Martin Lodge call the "prototype regulation," the public interventions that are "intentional and direct."[53] Instead, they adopt a far higher level of abstraction, seeing regulation as a varied set of "mechanisms of social control."[54]

---

[49] Matthew Schaefer, *The Need for Federal Preemption and International Negotiations Regarding Liability Caps and Waivers of Liability in the U.S. Commercial Space Industry*, 33 BERKELEY J. INT'L. L. 223, 230 (2015).

[50] *Id.* at 231.

[51] *Id.* at 233–34. Note that the government may intervene in other ways. The government can promote international standards on liability through diplomacy. *Id.* at 242–44. The government can also legislate immunity from liability under certain circumstances. *See, e.g.*, *id.* at 254 tbl.1 (discussing legislation on immunity for space activities in Virginia, Colorado, Texas, New Mexico, California, and Florida).

[52] A READER ON REGULATION 3 (Robert Baldwin, Colin Scott, & Christopher Hood eds., 1998).

[53] Christel Koop & Martin Lodge, *What is Regulation? An Interdisciplinary Concept Analysis*, 11 REG. & GOVERNANCE 95, 105 (2017).

[54] A READER ON REGULATION, *supra* note 52, at 4.

The section below offers a non-exhaustive summary of four of the key insights that scholars in this area have promulgated around technological regulation. It includes the intersection between technology and classification, technology and the regulator, and technology and globalization. When we think about insurance regulation, specifically the regulation of insurance for evolving technologies, we might benefit from exploring these insights.

A. TECHNOLOGY AND CLASSIFICATION

New technologies "may take earlier regulations by surprise."[55] These technologies introduce new risks and reduce old ones; they trigger new activities, and thereby fall into "regulatory lacunae" or "present regulatory misfits."[56] Underlying all of these is the sense that "emerging technologies challenge existing regulatory paradigms."[57] Indeed, both judge-made common law and statutory regulation depend on categorizations that evolve over time. In this regard, rule-appliers might be tempted to fit square pegs into round holes. Law-and-technology scholars highlight the fact that any such legal categorization is a mere "construct" where "the dispute and context are the immutable reality."[58] As such, "[i]f legal categories do not fit a new reality well, then it is the legal categories that must be re-evaluated."[59]

Insurance law has its own set of traditional classifications. Insurers often rely on "classification criteria" in the "marketing, underwriting, and pricing" stage.[60] These are a set of "factors insurance companies use to assign individual applicants to groups differing in riskiness for the purpose

---

[55] Anupam Chander, *Future-Proofing Law*, 51 U.C. DAVIS L. REV. 1, 15 (2017).

[56] *Id.*

[57] *Id.* at 16. *See also* Gregory N. Mandel, *Legal Evolution in Response to Technological Change*, *in* LAW, REGULATION, AND TECHNOLOGY 225, 227 (Roger Brownsword, Eloise Scotford, & Karen Yeung eds., 2017) (noting three lessons that are "generalizable cross a wide variety of technologies, legal fields, and contexts. These three lessons are: (1) pre-existing legal categories may no longer apply to new law and technology disputes; (2) legal decision makers should be mindful to avoid letting the marvels of new technology distort their legal analysis; and (3) the type of legal disputes that will arise from new technology are often unforeseeable." (citation omitted)).

[58] Mandel, *supra* note 57, at 234.

[59] *Id.*

[60] Regina Austin, *The Insurance Classification Controversy*, 131 U. PENN. L. REV. 517, 517 (1983).

of determining whether insurance will be sold to them, and, if so, at what cost and on what terms."[61]

New technological risks might result in breaking away from paradigmatic insurance classifications. Take for example the size of a company. Oftentimes, size is a useful category for determining the nature and scope of a risk posed by a prospective client. But in the cyber insurance domain, small companies could pose significant risk for cyber incidents (e.g., a business model that centers around the collection and transfer of large volumes of personally identifiable information),[62] whereas a large company might pose a minimum risk.[63]

When addressing new technological risks, insurers frequently use technology as well. The use of insurtech and lawtech tools open the door for predictive analysis and the ability to mine vast data troves to provide insights into the actuarial process.[64] Insurers and reinsurers alike "can better clean and process their data and identify indicators for known and unknown

---

[61] *Id.*

[62] *See* Eric Chabrow, *Cyber-Insurance: One Size Doesn't Fit All*, SEC. AGENDA, Mar. 2013, at 14, 15, https://fa94d5c47256403c613d-7164cafcaac68bfd3318486ab257f999.ssl.cf1.rackcdn.com//security-agenda-re-assessing-risk-evolving-threats-require-new-approach-to-risk-management-pdf-h-41.pdf (Citing Kevin Kalinich, global network and cyber-risk practice leader for Aon Risk Solutions, an insurance brokerage, who said that "[t]o the extent that an entity has a large number of personally identifiable information records, then there's a much bigger chance of exposure.").

[63] *Cf.* OECD REPORT, *supra* note 5, at 74 ("Insurance companies also focus significant attention on the company's security practices and policies, depending on company size and amount of coverage being sought. For smaller companies/coverage amounts, the underwriting process will focus on basic cyber security practices such as use of a firewall, anti-virus/malware software and data encryption, as well as frequency of data backups and use of intrusion detection tools.")

[64] *See* Agnieszka McPeak, *Disruptive Technology and the Ethical Lawyer*, 50 U. TOL. L. REV. 457, 461–68 (2019) (discussing lawtech). *See, e.g.*, Gina Clarke, *How Your Insurance Quote Is Powered by Artificial Intelligence*, FORBES (Jan. 21, 2019, 6:50 AM), https://www.forbes.com/sites/ginaclarke/2019/01/21/how-your-insurance-quote-is-powered-by-artificial-intelligence; *How Strong Is the Impact of Artificial Intelligence in the Insurance Industry?*, MEDIUM: INMEDIATE.IO (Aug. 1, 2019), https://inmediatesg.medium.com/how-strong-is-the-impact-of-artificial-intelligence-in-the-insurance-industry-34bd93ad47ac.

risks."[65] Indeed, machine learning "can recognize patterns that human underwriters never thought to investigate, or those that correlate with risk so subtly that they were not previously identified."[66] Insurers may also integrate technology throughout their business by encouraging clients to wear connected devices and place advanced sensors in their vehicles or on their networks.[67] Such "trove of personal data and corresponding analytics" may be used to "limit major risks before they occur,"[68] personalize insurance offerings,[69] engage in continuous underwriting,[70] and detect insurance fraud more easily.[71]

At the same time, however, "[t]he iterative, unsupervised analysis used by AI to price insurance policies may undermine the limited state and federal protections that exist to protect vulnerable groups and suspect classes from higher prices."[72] This adds to a growing list of potential inequalities that could emerge from an overutilization of technology for insurance marketing purposes, including: algorithmic bias, data harvesting, privacy intrusions, insurance data breaches, and ultimately discrimination.[73] Anya Prince and Daniel Schwarcz have, for example, demonstrated how the use of

---

[65] Jennifer Coleman, *Risk Management Implications and Applications of Artificial Intelligence Within the (Re)Insurance industry*, *in* THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE (RE)INSURANCE SECTOR 19 (SCOR SE ed., 2018), https://www.scor.com/en/download/file/25130?token=def50200e8f41bdba1037e4db3993f17964956470fd96275cfcbc2b7217828b4cba870aa6bc069b54009f44ccf32ee1e13328782e368382e06b2b64cc7fdeb1a566931b95cbcd7177e5dbbf09fc5d7bd8d8860761dbe1e7eb83a4eddf4017ce3ef74840f1e3f67e4dc1cd03727ef1d146f3474a76fa310f66b755c9589b2e40f8ed80ddea9.

[66] Samuel Lewis, *Insurtech: An Industry Ripe for Disruption*, 1 GEO. L. TECH. REV. 491, 494 (2017).

[67] *Id.* at 494–95. *See also* Yehonatan Shiman, *Expected Bad Moral Luck*, 25 CONN. INS. L.J. 112, 149 (2018) (noting that insurtech based "underwriting procedures rely on information gathered through mass-data collections from smart-phones, web searches, wearable sensors, and meta-data, among others to make better-informed decisions about an applicant's risk level. Access to this information's quantity and quality better positions insurance companies to assess risk, set representations and warranties, as well as mitigate exposure to moral hazard and fraud." (footnotes omitted)).

[68] Lewis, *supra* note 66, at 494.

[69] *Id.* at 495–96.

[70] *Id.* at 496–97.

[71] *Id.* at 497.

[72] Rick Swedloff, *The New Regulatory Imperative for Insurance*, 61 B.C. L. REV. 2031, 2058 (2020).

[73] *See generally id.* at 2057–70.

AI by insurance would inevitably result in "proxy discrimination" which could prove an "increasingly fundamental challenge to anti-discrimination regimes."[74] In other words, the use of these technologies by insurance agencies could by itself introduce new regulatory challenges and complicate existing legal classifications.

B. TECHNOLOGY AND THE REGULATOR

Rebecca Crootof and B.J. Ard introduce a methodological framework for rule-appliers and rule-prescribers in structuring their responses to what they call "TechLaw" questions.[75] The framework may be summarized in the following three-pronged analysis.

First, the assessor is called to "[i]dentify the type(s) of legal uncertainty at issue with regard to an artifact [new technology], [tech-enabled] actor, or activity [tech-enabled conduct]."[76] In this phase, the assessor will explore three questions: (a) "[w]hether and how existing law applies" (and what legal gaps and overlaps might have been erected); (b) "[w]hether existing law accomplishes its intended aims" (and in what ways might it be under or over inclusive); and (c) "[w]hether existing legal institutions have the authority, competence, or legitimacy to resolve applications and normative uncertainties."[77]

Second, the assessor is asked to "[e]valuate [the technology's] potential benefits and risks" and "consider who is likely to be impacted and their ability to mobilize for change."[78] Based on this information, the assessor might adopt a permissive approach (a "[p]resumption favoring less regulation" where the "tech's opponents bear [the] burden of changing law") or a precautionary approach (a "[p]resumption favoring preemptive regulation" where the "tech's proponents bear [the] burden of changing law).[79]

At the final stage, the assessor "determine[s] which response(s) will best resolve the [tech-fostered] legal uncertainty."[80] The assessor may

---

[74] Anya E.R. Prince & Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 IOWA L. REV. 1257, 1264 (2020).

[75] Rebecca Crootof & BJ Ard, *Structuring TechLaw*, 34 HARV. J.L. & TECH. 347, 350 fig.1 (2021) (providing an illustration of their methodological framework).

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] *Id.*

[80] *Id.*

choose to "[e]xtend [e]xtant [l]aw," "[c]reate [n]ew [l]aw," or "[r]eassess the [r]egime."[81]

This analytical roadmap is extremely useful, even from the perspective of a regulator looking to regulate a new insurance market for technological risk. It provides a useful canvas and set of factors that each assessor may look at to evaluate at different junctures throughout the life cycle of the technology and as disputes arise. Nonetheless, the framework stops short of providing immediate answers to three follow-up questions: who, when, and what.

1. Who?

Who should be the assessor? Local, state, or federal legislatures and courts? State insurance regulators and attorney generals, or federal administrative and enforcement agencies? Or what about international organizations and foreign governments? What is clear to me is that the regulation of technological risk and the insurance markets associated with it requires a reconceptualization of the old McCarran–Ferguson dichotomy. The 1945 Act, passed by the 79th Congress, sought to exempt the business of insurance from most federal regulation.[82] But to think of insurance regulation in such a narrow way is unpersuasive.

The assessor or regulator can be different entities, at different times, depending on the situation. Whoever is the assessor must be mindful of their institutional capacities and pitfalls. They should be cautiously aware of the limits of their authority and the long-term consequences that a poorly made decision could have on the continued evolution of the market.

Consider, for example, the management of insurance policy language. Legislatures and regulators are far superior to courts in this area.

> The legislative and regulatory processes allow prospective implementation of changes to policy language and prospective calculation of premiums based on risks assumed by the insurer. Modifications to agreements through the judicial process, however, are primarily retrospective, long

[81] *Id.*

[82] McCarran–Ferguson Act, 15 U.S.C. §§ 1011–1015 (1945).

> after the contracts were entered into and premiums calculated and paid based on agreed-to policy language.[83]

Moreover, many insurance policies, in an attempt to future-proof their language, incorporate into their text the evolving regulation by the legislator. For example, directors and officers liability policies often include an exclusion for:

> [A]ny actual or alleged violation of any securities law, regulation or legislation, . . . any other federal securities law or legislation, or any other similar law or legislation of any state, province or other jurisdiction, or any amendment to the above laws, or any violation of any order, ruling or regulation issued pursuant to the above laws . . . .[84]

In this regard, any regulator needs to understand that by amending or extending laws, they are directly injecting themselves into the bilateral contracts between insurers and insureds, who take their cues directly from the legislation. Since "legal liability for [c]yber [r]isk is rapidly and constantly evolving,"[85] in part through state legislation and enforcement agency action, cyber insurance is particularly susceptible to this phenomenon.

But state regulation also has its limits. As Daniel Schwarcz and Steven Schwarcz have shown, "[s]tate insurance regulation is poorly equipped to address systemic risk in insurance . . . ."[86] This is due, in part, to the fact that "[d]elegating to States sole regulatory responsibilities over

---

[83] Prodigy Commc'ns Corp. v. Agric. Excess & Surplus Ins. Co., 288 S.W.3d 374, 387 (Tex. 2009) (Johnson, J., dissenting).

[84] BEAZLEY, INFORMATION SECURITY & PRIVACY INSURANCE WITH ELECTRONIC MEDIA LIABILITY COVERAGE FORM F00106SL 7 (Aug. 2011 ed., 2011), https://www.beazley.com/documents/Private%20Enterprise/Wordings/NEW%202011%20Info%20Sec%20Form%20F00106SL%20082011%20ed.pdf.

[85] 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, 406 (2015)

[86] Daniel Schwarcz & Steven L. Schwarcz, *Regulating Systemic Risk in Insurance*, 81 U. CHI. L. REV. 1569, 1627 (2014). The second reason for why states tend to underperform when regulating systemic risk (beyond the "internalization principle") is the fact that state regulators "lack the necessary expertise and perspective." *Id.* at 1631. State insurance regulators are also lacking in their ability to coordinate together and with the federal government. *Id.* at 1632.

activities that produce negative externalities nationally or internationally will generally lead to underregulation of those activities."[87] Since certain cyber risks are systemic, due to common vulnerabilities and concentrated dependencies that could lead to cascading effects,[88] states cannot possibly regulate cyber insurance alone.

But it is not just states. National governments cannot be the sole insurance regulators of technological risk. Neil Doherty once wrote that the "long delays between the writing of the [insurance] contract and the realization of loss permit a substantial cumulative change in the information base" on which the policy was formulated and priced.[89] Doherty noted that "[t]hese changes arise both from legislative and judicial changes in liability rules and from judicial precedents which re-interpret insurance contract wordings."[90] As technology is not always limited by territorial line drawing, the legislative and judicial changes might occur overseas and have ripple effects at home. Examples of such international changes include: an international treaty on cyber attribution; new cybersecurity best practices from the International Standard Organization ("ISO"); changes to privacy policies promulgated by a European national data protection authority; or revised understanding of common cyber insurance clauses developed by the International Underwriting Association or Lloyd's Market Association.[91]

Moreover, the changes in the "information base" that Doherty spoke of, which impact the risk environment, can also be non-legislative and non-

---

[87] *Id.* at 1628.

[88] DAVIS HAKE, ANDREAS KUEHN, ABAGAIL LAWSON & BRUCE MCCONNELL, CYBER INSURANCE AND SYSTEMIC MARKET RISK 5 (2019), https://www.eastwest.ngo/sites/default/files/ideas-files/cyber-insurance-and-systemic-market-risk.pdf. *See also* Abraham & Schwarcz, *supra* note 9, at 11 (discussing "damage risk," "liability risk," and "coverage risk," as three prerequisites for a cyber catastrophe that could result in correlated losses for insurers).

[89] Neil A. Doherty, *The Design of Insurance Contracts When Liability Rules are Unstable*, 58 J. RISK & INS. 227, 243 (1991).

[90] *Id.* at 243–44.

[91] One example of this can be seen in the context of extraterritorial data protection legislation, such as the European General Data Protection Regulation (GDPR). *See* Commission Directive 16/679, 2016 O.J. (L 119) 1 (EU). *See also* ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD 142 (2020) (introducing a "Brussels Effect" as an example for utilizing European market power to force foreign corporations to comply with European data protection standards. Bradford cites to others who have described the GDPR as "unashamedly global." She notes that given both the fact that the regulation is "extraterritorial and highly inelastic" and the fact that abandoning the EU market "is not even remotely a commercially viable option" results in the EU's expansive regulatory capacity.).

judicial. They may be societal. As society discovers new technology and employs it in ways not first imagined or envisioned by its creators, the technology takes on a life of its own. What it means to be safe or negligent, efficient or inefficient, tortious or innocent, will evolve over time. They will be shaped by social customs and intuitions formed around the technology.[92] This may be a slow and incremental process, or, depending on the technology, could also rapidly move alongside technology's deployment and adoption. If private law and private ordering "draw from and reinforce social norms,"[93] as Merill has suggested, then a broader set of actors could be seen as potential norm-developers, and therefore possible regulators of this liability and insurance environment. From design decisions made by technology companies to influencers on TikTok, our collective understating of custom around new technologies will be shaped by an ecosystem larger than one state insurance regulator.

2. When?

A complex set of questions goes into deciding when to introduce a new law into a technologically evolving environment.[94] Sometimes, simply letting the market run its course can prove to be the more efficient route. Consider this historical example:

> In ancient China mandarins who ran espionage operations devised what they believed was a foolproof secret

---

[92] João Marinotti notes that even in the context of emerging and disruptive technologies, shared "social customs and intuitions can stem from cognitive effects of human perception, as well as from learned associations, whether economic, social, or otherwise." João Marinotti, *Tangibility as Technology*, 37 GA. STATE U. L. REV. 671, 709 (2021) (footnotes omitted).

[93] Thomas W. Merrill, *Private and Public Law*, *in* THE OXFORD HANDBOOK OF THE NEW PRIVATE LAW 575, 578 (Andrew S. Gold, John C.P. Goldberg, Daniel B. Kelly, Emily Sherwin & Henry E. Smith eds., 2021). *See also* Nathan B. Oman, *Private Law and Local Custom*, *in* THE OXFORD HANDBOOK OF THE NEW PRIVATE LAW 159, 172–74 (Andrew S. Gold, John C.P. Goldberg, Daniel B. Kelly, Emily Sherwin & Henry E. Smith eds., 2021) (referring to the "prevailing beliefs and practices of the community" as a source for of private law rules, further noting that courts "fit the law to the character of their particular community, with an eye to its institutions and historical development.").

[94] Colin B. Picker, *A View from 40,000 Feet: International Law and the Invisible Hand of Technology*, 23 CARDOZO L. REV. 149, 203–05 (2001) (outlining questions for policymakers crafting international regulations for new technologies).

> communication system for spies. They shaved a spy's head, wrote a secret message on the bald skull, then waited until the spy's hair grew back, at which point he would be sent on his way. At his destination his head would be shaved again, revealing the message.[95]

If we were rule-prescribers living at that time and were worried about espionage, we might rush into setting some rules of the road for the emerging practice of "skull messaging."

Instead, we could also wait. As Jonathan Zittrain observed, "[t]he procrastination principle rests on the assumption that most problems . . . can be solved later or by others."[96] Indeed, in our historical example, the obvious was soon realized—that the months of delay required before a new set of hair grew, made the communication itself quite futile.[97]

It was this deficiency in the system that made the Greeks in 480 BCE devise the scytale as an alternative.[98] The scytale "involved writing on the length of a sheet of papyrus wound around a staff, which, when removed and sent on, was intelligible only to a recipient who had a twin staff of precisely the same diameter and length."[99] Of course, the scytale was only useful for short messages. The need to write longer secret communications is what eventually led to the discovery of invisible ink.[100]

Round and round we go as needs trigger innovation and user feedback triggers new needs, which in turn trigger new innovations. Rule-prescribers must choose wisely the right moment for a regulatory intervention in this otherwise closed loop. At the same time, they might benefit from not waiting too long. Early interventions could provide "a more

---

[95] ERNEST VOLKMAN, THE HISTORY OF ESPIONAGE: THE CLANDESTINE WORLD OF SURVEILLANCE, SPYING AND INTELLIGENCE, FROM ANCIENT TIMES TO THE POST-9/11 WORLD 20 (2007).

[96] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET – AND HOW TO STOP IT 31 (2008). *See also* Yoram Dinstein, *The Recent Evolution of the International Law of Armed Conflict: Confusions, Constraints, and Challenges*, 51 VAND. J. TRANSNAT'L L. 701, 710 (2018) (suggesting that in the context of the introduction of AI to the battlefield and the "awesome conundrums" that such a weapon system introduces, "answers should lie in wait until we have a much better picture of what the technology will actually look like.").

[97] VOLKMAN, *supra* note 95, at 20 ("[I]t takes time for a full head of human hair to grow back, meaning any intelligence on that skull cannot be very timely.").

[98] *Id.*

[99] *Id.*

[100] *Id.*

objective regulatory atmosphere, before parties become entrenched and adversarial. In contrast, deferring action (usually in the name of preserving discretion and gathering information), often leads to incremental decision making, which is more susceptible to interest group influence."[101]

This tension has perfectly manifested itself in the intellectual exchange between Ryan Calo, Kenneth Abraham, and Robert Rabin with regards to autonomous vehicle liability and insurance regulation. On one side stands Calo, who claims that no one holds a "crystal ball" and that the "very prospect that dramatically distinct modalities of transportation could arise from the ability of vehicles to drive themselves seems to caution against a preemptive, administratively intense solution that forbids state legislatures or courts from experimentation."[102] On the other side stand Abraham and Rabin. As autonomous vehicles "are already on the roads being tested," they posit that "[w]e cannot afford to wait and see what the future brings over a period of decades . . . ."[103] The future, they say, "is just over the horizon. The failure to do something about that is not the equivalent of keeping our policymaking powder dry."[104]

Timing is everything in life and in law. As the book of *Ecclesiastes* teaches "[t]o every [thing there is] a season, and a time to every purpose . . . ."[105] Therefore, different kinds of regulations by different kinds of regulators will be appropriate at different times. It is therefore possible that Calo, Abraham, and Rabin are all correct in thinking that some regulations may be good for now, while others might be good for later.

3. What?

In the age of technological innovation, rulemaking can take different forms. "Many agencies regularly employ a mix of policymaking tools on a given issue—sometimes promulgating or amending a rule, sometimes bringing an enforcement action, and sometimes issuing a guidance document."[106] To increase opportunities for trial-and-error, innovation, and flexibility, regulations can be further experimented with. One type of forum

---

[101] Nathan Cortez, *Regulating Disruptive Innovation*, 29 BERKELEY TECH. L.J. 175, 204 (2014).

[102] Calo, *supra* note 1, at 87.

[103] Kenneth S. Abraham & Robert L. Rabin, *The Future is Almost Here: Inaction is Actually Mistaken Action*, 105 VA. L. REV. ONLINE 91, 92 (2019).

[104] *Id.*

[105] *Ecclesiastes* 3:1 (King James).

[106] M. Elizabeth Magill, *Agency Choice of Policymaking Form*, 71 U. CHI. L. REV. 1383, 1410 (2004).

for this kind of legal incubation is the "regulatory sandboxes"– environments in which regulation can be pre-tested in a relative vacuum with real stakeholders.[107] In such a scenario, co-regulation becomes possible as collaboration is fostered between the regulator and the regulated entity.[108] In the context of cyber insurance, Israel is now attempting to become a national sandbox, a beta site for experimentation in cyber insurance regulation.[109]

Regulation does not only mean formal prescriptive top-to-bottom ordinances. Formal legal rules are but one of four types of constraints that "regulate" in the broader sense. Lawrence Lessig identified the three other constraints as, "social norms, the market, and architecture."[110] I have already elaborated on the importance of social customs and intuitions in private law and private ordering,[111] so I will briefly address the two remaining constraints.

Price points, supply-and-demand, and barriers to accessibility will impact behavior. Combined with other soft law instruments, such as "private standards, codes of conduct, certification programs, principles, guidelines, and voluntary programs,"[112] these form market constraints on the technology, which in turn shape our expectations around its functions, properties, and limits.

Choices in the design and architecture of a technology will also impact our collective understanding of its features and capacities. As noted by Paul Ohm and Blake Reid, "[w]e used to regulate things, and now we regulate code."[113] João Marinotti has shown, for example, how the

---

[107] Hilary J. Allen, *Regulatory Sandboxes*, 87 GEO. WASH. L. REV. 579, 579 (2019).

[108] For further reading on regulatory sandboxes see *id.*; Radostina Parenti, *Regulatory Sandboxes and Innovation Hubs for FinTech Impact on Innovation, Financial Stability and Supervisory Convergence, Study for the Committee on Economic and Monetary Affairs*, POL'Y DEP'T. ECON. SCI. & QUALITY LIFE POL'Y, PE 652.752, 33–38 (Sept. 2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652752/IPOL_STU(2020)652752_EN.pdf.

[109] *See* Asaf Lubin, *Cyber Insurance as Cyber Diplomacy*, *in* CYBER WAR & CYBER PEACE IN THE MIDDLE EAST: DIGITAL CONFLICT IN THE CRADLE OF CIVILIZATION 22, 27–30 (Michael Sexton & Eliza Campbell eds., 2020).

[110] LAWRENCE LESSIG, CODE: VERSION 2.0 123 (2006).

[111] *See supra* notes 92–93 and accompanying text.

[112] Gary E. Marchant, *Governance of Emerging Technologies as a Wicked Problem*, 73 VAND. L. REV. 1861, 1866 (2020).

[113] Paul Ohm & Blake Reid, *Regulating Software When Everything Has Software*, 84 GEO. WASH. L. REV. 1672, 1702 (2016).

"cryptographic imperatives"[114] of exclusion and control, which are embedded in the core of Bitcoin, resulted in the "establishment of a shared social custom and intuition about how bitcoins are used and what non-owners may or may not do."[115] In other words, the architecture of the technology helps regulate the legal interests and liabilities that emerge from and in response to a volatile technological space.

All of these demonstrate that when we wish to engage in the regulation of an evolving technology, say around its liability and insurance, we must adopt a broader lens. There can be different regulated entities. For example, we may think about the regulation of insurers, or of the insured; we may regulate tech providers, or their clients; we may limit our regulation to public entities, or extend it to private entities; we may focus on large corporations or particular sectors; or we may adopt a whole-market approach, including small-to-medium enterprises.

Applying these concepts in the cyber insurance context, we may be able to develop a non-exhaustive list of potential examples of both direct and indirect regulations that may be employed by different kinds of regulators at different times. What distinguishes these two categories is that whereas direct regulations target the commercial insurers themselves, indirect regulations target the legal and policy environment in which these insurers operate.

Illustration 2: Examples of Different Initiatives for Direct and Indirect Cyber Insurance Regulation

Direct Regulation	**Indirect Regulation**
Cyber Claims Information-Sharing Requirements	Data Breach Notification Laws
Security Data Depositories	State/Federal/Foreign Privacy and Data Protection Regulation
Mandatory Policy Language or Questionnaires	Subsidies for Cybersecurity Services and/or Research and Development
Governmental Insurance of Last Resort for State-Sponsored Cyber Operations and Other Acts of Cyber War or Terrorism	Cybersecurity Liability Safe Harbor Laws

[114] Marinotti, *supra* note 92, at 726.
[115] *Id.* at 728.

Direct Regulation	Indirect Regulation
Prohibition on Ransomware Payments	Liability for Tech Providers (e.g., Internet-of-Things Vendors)
Prohibition on Indemnification of Statutory Data Protection Fines	Government Exercise of its Procurement Power to Support Cybersecurity Best Practices
Standard Metrics, Requirements, and Other Data Formats for Assessment or Claims Process	National Certification of Cybersecurity Standards and Licensing of Cybersecurity Providers
Establish Insurer Liability for Providing Security Advice	International Frameworks for Cybersecurity Attribution
Make Cyber Insurance Compulsory for Certain Industries	Rules of International Law on Responsible Behavior in Cyberspace

C. TECHNOLOGY AND GLOBALIZATION

Technology, in the sense of human innovation and human progress, is a phenomenon that defies national borders. Technology has a tendency to spread and connect individuals in ways that go beyond jurisdictional lines. "A regulator sitting in Washington, D.C. considering how to approach a new technology must keep in mind that her counterpart in Brussels, Beijing, or Bogota is likely pondering the same question. She has to make decisions to regulate or not, or how to regulate, while looking over her shoulder."[116]

This lesson is particularly acute in the context of cyber insurance. This is because cybersecurity and cyber stability are matters of national and international security, and therefore are matters that are intimately connected to global political affairs. Espionage operations by a foreign nation state, like the SolarWinds hack, could have cascading effects on the markets.[117] As such, what is discussed in the United Nations Security Council in the morning may end up on the table of a commercial insurer in Connecticut by evening time. Few other insurable risks share this property. Put differently, if the Ace American Insurance Company is truly concerned with whether its wartime exclusion applies in the case of an alleged Russian ransomware

[116] Chander, *supra* note 55, at 21.

[117] For more on the SolarWinds Hack see Asaf Lubin, *SolarWinds as a Constitutive Moment: A New Agenda for the International Law of Intelligence*, JUST SEC. (Dec. 23, 2020), https://www.justsecurity.org/73989/solarwinds-as-a-constitutive-moment-a-new-agenda-for-the-international-law-of-intelligence/.

attack,[118] it should focus its advocacy not only in the courts of New Jersey but also at conferences in Geneva.

As I have written elsewhere, cyber insurance should be seen as a form of cyber diplomacy, as we aim to promote globally coordinated, nuanced, and effective regulation.

> If cyber diplomacy is truly concerned with enhancing cyber deterrence and promoting norms that ensure global cyber stability and cyber peace, it must broaden its perspective to include international insurance norms for modeling and indemnifying the perils of cyberspace.
>
> . . . .
>
> In an effort to expand the multi-stakeholder understanding of the risks cyber threats pose to society, we must begin to draw additional actors into the fold. Involving commercial reinsurers and insurers, brokers, underwriters, cyber risk insurance pool directors, corporate chief cyber risk officers, and insurance law and policy scholars and think-tanks in a larger conversation about the future of international cybersecurity would be a pivotal first step toward a more democratic and inclusive dialogue. Such a dialogue would offer more nuanced solutions to practical challenges, and would ensure better norm design by the very actors that will ultimately be tasked with ensuring the norms' proper implementation.[119]

---

[118] On December 6, 2021, the Superior Court of New Jersey granted Merck & Co.'s motion for partial summary judgment against Ace American Insurance Co. and denied the insurer's cross-motion. Merck & Co. v. Ace Am. Ins. Co., No. UUN-L-2682 at 8 (N.J. Super. Ct. Law Div. Dec. 6, 2021) (Bloomberg Law, Court Dockets). After examining both the plain language of the property insurance policy and the applicable caselaw surrounding the hostile/warlike exclusion, the Court concluded that the NotPetya cyberattack, allegedly launched by Russian officials, did not trigger the exclusion. *Id.* at 11. For a broader discussion of the topic and analysis of related attribution and international law matters see Scott J. Shackelford, *Wargames: Analyzing the Act of War Exclusion in Insurance Coverage and Its Implications for Cybersecurity Policy*, 23 YALE J. L. & TECH. 362 (2021).

[119] Lubin, *supra* note 109, at 24, 32 (footnotes omitted).

III. THE ROLE OF GOVERNMENT IN FOSTERING CYBER INSURANCE

With all this knowledge we may now come back to the question posed by the organizers of *A Cyber Cyber Insurance Conference*: what can, and should, state and federal governments do to promote more robust cyber insurance markets? To focus our analysis, let us look at one possible regulation: the recent New York Cyber Insurance Framework, the first of its kind in the country. The following section will assess the promise and limits of this framework and then offer broader observations about the future of cyber insurance regulation.

A. THE NEW YORK CYBER INSURANCE FRAMEWORK

On February 4, 2021, the New York Department of Financial Services ("NY DFS"), led by Superintendent Linda Lacewell, introduced the first state-wide cyber insurance regulation in the United States.[120] The circular, titled *Cyber Insurance Risk Framework*,[121] begins with a bombastic statement. Weaving together the impacts of COVID-19 on remote working, the rise of ransomware attacks, and the recent SolarWinds cyber-espionage campaign, it makes the case for such a state-wide intervention. The circular is thus meant to "foster the growth of a robust cyber insurance market that maintains the financial stability of insurers and protects insureds."[122]

The circular is the result of an "ongoing dialogue with the insurance industry and experts on cyber insurance," including meetings with "insurance regulators across the U.S. and Europe."[123] It identifies "systemic risk" and "silent risk" (what is known as non-affirmative cyber coverage) as two of the biggest challenges for managing cyber insurance, alongside the general challenge of dealing with the growing threat of cybercrime, in particular in the form of ransomware attacks.[124]

The framework applies only to "authorized property/casualty insurers [licensed in New York] that write cyber insurance."[125] The framework centers around seven practices that are to be employed by the

---

[120] Letter from Linda A. Lacewell, *supra* note 25.

[121] *Id.*

[122] *Id.*

[123] *Id.*

[124] *Id.* (citing a 180% increase in ransomware insurance claims suggesting that ransomware is a $20 billion problem).

[125] *Id.*

insurers to "sustainably and effectively manage their cyber insurance risk."[126] The circular does note that each insurer's risk portfolio will vary on the basis of their "size, resources, geographic distribution, market share, and industries insured."[127] As such, the framework seems to offer a general and flexible model, subject to specific interpretation by each insurer. On the one hand, such flexibility allows for the kind of experimentation in regulation that I have argued is positive as the insured risks continue to evolve. On the other hand, such open-ended regulation could also result in a difficultly to enforce the standards, which could lower the regulation's overall effectiveness. The seven practices insurers should employ are:

> (1) "Establish a Formal Cyber Insurance Risk Strategy;"
> (2) "Manage and Eliminate Exposure to Silent Cyber Insurance Risk;"
> (3) "Evaluate Systemic Risk;"
> (4) "Rigorously Measure Insured Risk;"
> (5) "Educate Insureds and Insurance Producers;"
> (6) "Obtain Cybersecurity Expertise;" and
> (7) "Require Notice to Law Enforcement".[128]

There is obviously a lot of good intention here. The NY DFS should be commended for taking such a bold initiative at a time where few government regulators and legislatures (be it local, state, or federal) seem keen to enter the fray. It also targets some really low-hanging fruit, by formalizing the need of insurers to establish a cyber insurance risk strategy, retain qualified personnel, and obtain cybersecurity expertise, including through the use of outside providers and vendors. As one commentator noted, these are "both obvious and eye opening."[129] If there were any cyber insurers who were still unaware of these basic requirements, the circular might serve as a much-needed wakeup call and could help "create new incentives and pre-incident programs."[130] To the very least the circular helps codify a certain set of industry practices and general standards, which by itself is an important contribution, one that could be mimicked by other state regulators.

---

[126] *Id.*

[127] *Id.*

[128] *Id.*

[129] Joshua Mooney, *Breaking Down New York's Department of Financial Services' New Cyber Insurance Framework*, KENNEDYS L. (Feb. 18, 2021), https://kennedyslaw.com/thought-leadership/article/breaking-down-new-york-s-department-of-financial-services-new-cyber-insurance-framework/.

[130] *Id.*

Nonetheless, the circular suffers from significant ambiguity and uncertainty, further demonstrating the limits of one state regulator's authority and power in tackling such a massive undertaking. Within the limits of this paper, I will demonstrate four core challenges with the current framework.

First, why focus only on "authorized property/casualty insurers that write cyber insurance?"[131] In so doing, the circular seems to neglect both those insurers who do not explicitly write cyber insurance, as well as other insurers outside the property/casualty world. All these insurers might still be engulfed by the challenges of silent cyber coverage, yet the policy seems to target a very limited group.[132] As I have demonstrated above, asking who should be regulated, and in what ways, is one of the first challenges for every assessor.

Second, the framework "can inspire competing reactions as it signals incoming mandates that hover on the horizon without offering much substance as to how to accomplish them."[133] Take, as one example, the issue of "systemic risk." The circular calls on insurers to assess this risk, even citing the specific concern of supply-chain attacks as a possible vector in this regard.[134] But the circular falls short of actually providing insurers with specific tools, resources, or even general frameworks to conduct such analysis. As we have already seen, systemic risk is one of the areas where state insurers are way over their heads. Similarly, requiring insurers to develop "qualitative and quantitative goals for risk"[135] as part of a cyber insurance risk strategy and calling on them to "obtain cybersecurity expertise"[136] does not mean much if the state is not also willing to assist those insurers who need it by providing actual resources, actuarial techniques, specific recommended security controls, and even subsidies to certain industries or public entities, to accomplish these efforts.[137]

---

[131] Letter from Linda A. Lacewell, *supra* note 25.

[132] Thanks to Kenneth S. Abraham for pointing out this concern during the *A Cyber Cyber Insurance Conference*.

[133] Mooney, *supra* note 129.

[134] Letter from Linda A. Lacewell, *supra* note 25.

[135] *Id.*

[136] *Id.*

[137] As it currently stands, most commercial insurers do not possess "conclusive data on the effectiveness of cybersecurity controls and practices" nor are they well positioned at this time to "acquire and maintain a level of technical knowledge and expertise to advise on control selection and implementation conditioned on specific entity's security posture." DEP'T HOMELAND SEC., ASSESSMENT OF THE CYBER INSURANCE MARKET 15 (2019), https://www.cisa.gov/sites/default/files/publications/19_1115_cisa_OCE-Cyber-Insurance-Market-Assessment.pdf.

Third, the circular's only specific requirement—that policyholders notify law enforcement for ransomware attacks[138]—is also a source of some confusion. As a general matter, this is a policy that I have advocated for and makes a great deal of sense.

> [L]aw enforcement cannot carry out their duties, if they are not being informed of the hacks in the first place. There is a growing trend in cyber insurance policies to allow for ransomware extortion payment indemnification without requiring the policy holder to first notify the police or the FBI of the ransom prior to seeking compensation. Insurers argue that making such a demand to policyholders would disincentivize them from acquiring the policy in the first place, as they are worried about potential reputational harms. This collective action problem is resulting in a race to the bottom where it is enough for one insurer to avoid a requirement of notifying the FBI, for all insurers to follow suit out of worry of losing business.[139]

Nonetheless, one state regulator cannot tackle a collective action problem like this alone. The race to the bottom will continue if outside the state of New York, a failure to notify will continue to be the norm. This is a matter better left to federal regulation, not state. The circular is also silent as to the entity to be notified or scope of notification.[140] The reality is that the state is unable to actually enforce disclosure to federal law enforcement, over which it has no authority, nor can it be certain that the notification will be picked up and effectively handled once transmitted. A notification policy is only as good as the enforcement action that flows from it. As for local and state law enforcement, they are certainly in no position to manage the threat of global cybercrime and cyberwarfare, thereby highlighting the futility of notifying them.

Finally, a fourth challenge with the circular concerns the obligation to "rigorously measure insured risk" by focusing on a "data-driven" plan and "third-party sources."[141] In so doing, NY DFS seems to be going all-in

---

[138] Letter from Linda A. Lacewell, *supra* note 25.

[139] *See* Lubin, *supra* note 11, at 53–54.

[140] Letter from Linda A. Lacewell, *supra* note 25 (encouraging cyber insurance policies to include a requirement for victims to notify law enforcement but does not specify what law enforcement).

[141] *Id.*

on an AI-driven big-data insurtech solution. But the regulator fails to provide an actual list of preferred technologies, service-providers, or vendors. It leaves to the insurers the decision of who to contract with and in what ways, without even providing them the most limited set of considerations. Not all insurtech products are created equal, and different solutions could be more or less effective. Furthermore, as discussed, "the accelerating evolution of AI and big data render proxy discrimination a fundamental threat to important goals of many, if not most, antidiscrimination regimes."[142] The state fails to even acknowledge the myriad of ways by which the use of these tools could result in inequality, bias, privacy intrusion, and prohibited discrimination.

B. THE FUTURE OF CYBER INSURANCE REGULATION

For cyber insurance regulation, we must think outside the box. We need to adopt agility in the way we conceptualize the very concept of regulation. Understanding that the regulator, the regulated, and the regulation, can take different forms and occur at different times, is pivotal in developing a comprehensive and collaborative response to the contemporary threats and perils of cyberspace.

While insurance is traditionally viewed as a state-regulated market, the subject matter being insured, "cybersecurity," is certainly not. Insurers and insurance regulators should adopt a more holistic understanding of protections in cyberspace, recognizing that it is a domain ripe for complex public-private partnerships across a range of environments and frameworks.[143] Lessons from decades of U.S. regulation of privacy and data protection through a patchwork of sectoral and state initiatives (as opposed to an omnibus model in Europe) have led many scholars to call for federal and centralized regulation.[144]

---

[142] Prince & Schwarcz, *supra* note 74, at 1300.

[143] *See generally* JEFFREY BAXTER ET AL., ADDRESSING CYBER SECURITY THROUGH PUBLIC-PRIVATE PARTNERSHIP: AN ANALYSIS OF EXISTING MODELS 9 (Joseph Mazzafro ed., 2009), https://www.insaonline.org/wp-content/uploads/2017/04/INSA_AddressingCyber_WP.pdf (providing a "graphic and conceptual representation of a possible system for cyber security partnership"); Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467 (2017).

[144] *See, e.g.*, Daniel J. Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, TEACHPRIVACY: PRIV. + SEC. BLOG (Nov. 13, 2015), https://teachprivacy.com/problems-sectoral-approach-privacy-law/; Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL

The same could be applied here, precisely because of the unique features of cybersecurity as an evolving threat and the information asymmetries that accompany it. As such, no one state can handle cybersecurity risk on its own, just like no one insurer can cover this risk, especially if a mega cyber catastrophe occurs. In fact, recent trends have demonstrated precisely how unlikely it is that states and the market could handle this on their own. In the face of "skyrocketing" cyberattacks, including ransomware, insurers have begun to increase prices for cyber insurance products and denying coverage unless stringent controls are put in place.[145] As a result of that the market for primary cyber insurance "is really drying up."[146] In the face of these market shifts, only the federal government can effectively respond to and help fill this growing cyber insurance gap. An effective cyber insurance regulation will thus harness the commitment and dedication of state officials in a broader campaign co-led by national governments and the private sector.

CONCLUSION

As Rudyard Kipling masterfully opined in his 1943 poem, *The Secret of Machines*, the touch of technology can on occasion "alter all created things."[147] Emerging and evolving technologies introduce unique risks, harms, and regulatory challenges at different phases throughout each technology's life cycle. Against this background, rule-prescribers and rule-appliers have both a regulatory toolkit and a set of discretionary choices to make about the timing, scope, and nature of both prospective and reactive regulation. Commercial insurers play an important role in this narrative, both as private regulators of the technology they insure, and as a lobbying force to government in the formation of new regulations.

This paper has tried to demonstrate that there is value in exploring insurance regulation for emerging technologies through the broader lens of

---

ON FOREIGN RELS.: DIGIT. & CYBERSPACE POL'Y PROGRAM (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection; Joanna Kessler, *Data Protection in the Wake of the GDPR: California's Solution for Protecting "The World's Most Valuable Resource",* 93 S. CAL. L. REV. 99 (2019).

[145] Ian Smith, *Cyber Insurers Recoil as Ransomware Attacks 'Skyrocket'*, FIN. TIMES (June 2, 2021), https://www.ft.com/content/4f91c4e7-973b-4c1a-91c2-7742c3aa9922.

[146] *Id*. (quoting Graeme Newman, chief innovation officer of London-based insurance provider CFC).

[147] Rudyard Kipling, *The Secret of the Machines* (1943), *reprinted in* A CHOICE OF KIPLING'S VERSE 293, 294 (T.S. Eliot ed., 1973).

the law-and-technology literature. Law-and-technology scholars, who have mastered a comparative regulatory history of different technologies, in different locations, and at different times, might be able to teach us a thing or two about the way we should govern our technological insurance markets.

The reverse is, of course, also true. Law-and-technology scholars, by and large, focus much of their writing on the theory and practice of torts, contracts, property, criminal, constitutional, and administrative law. Rarely though, do these tech-minded academics engage in a deep dive into insurance. If we each step outside of our own silo and explore what the folks on the other side are writing and thinking about, we might be able to develop deeper and more nuanced insights.