THE TECHNOLOGIZATION OF INSURANCE: AN EMPIRICAL ANALYSIS OF BIG DATA AND ARTIFICIAL INTELLIGENCE'S IMPACT ON CYBERSECURITY AND PRIVACY

Shauhin A. Talesh[*] & Bryan Cunningham[**]

Abstract

This Article engages one of the biggest issues debated among privacy and technology scholars by offering an empirical examination of how big data and emerging technologies influence society. Although scholars explore the ways that code, technology, and information regulate society, existing research primarily focuses on the theoretical and normative challenges of big data and emerging technologies. To our knowledge, there has been very little empirical analysis of precisely how big data and technology influence society. This is not due to a lack of interest but rather a lack of disclosure by data providers and corporations that collect and use these technologies. Specifically, we focus on one of the biggest problems for businesses and individuals in society: cybersecurity risks and data breach events. Due to the lack of stringent legal regulations and preparation by organizations, insurance companies are stepping in and offering not only cyber insurance but also risk management services aimed at trying to improve organizations' cybersecurity profile and reduce their risk. Drawing from sixty interviews of the cyber insurance field, a quantitative analysis of a "big data" set we obtained from a data provider, and observations at cyber insurance conferences, we explore the effects of what we refer to as the "technologization of insurance," the process whereby technology influences and shapes the delivery of insurance. Our

[*] © 2021 Shauhin A. Talesh. Professor of Law, and by courtesy, Professor of Sociology and Criminology, Law & Society, University of California, Irvine. For helpful conversations and comments, we are grateful to Tom Baker, Dan Burk, Benjamin van Rooij, and Daniel Woods. We are grateful to those who participated in workshops at the American Bar Foundation, University of Pennsylvania Law School, University of California, Berkeley School of Law, Center for the Study of Law and Society, University of Maryland Socio-Technical Policy Institute, College of Information Studies, University of Minnesota and University of Connecticut Joint Conference on Cyber Insurance, and University of California, Irvine School of Law. Stephanie Lee, Hedyeh Tirgardoon, and Amruta Trivedi provided indispensable research support and the UCI law librarians kept us on track as usual. Support for this project was generously provided by the Herman P. and Sophia Taubman Foundation, UCI Beall Applied Innovation, and the UCI Cybersecurity Policy & Research Institute. We also thank insurance industry actors that allowed us to interview them.

[**] © 2021 Bryan Cunningham. Executive Director, Cybersecurity Research and Policy Institute, University of California, Irvine. Cybersecurity, Privacy, and Data Protection Attorney at Zweiback, Fiset & Coleman (https://zfclaw.com/); Former Deputy Legal Adviser to the White House National Security Council.

study makes two primary findings. First, we show how big data, artificial intelligence, and emerging technologies are transforming the way insurers underwrite, price insurance, and engage in risk management. Second, we show how the impact of these technological interventions is largely symbolic. Insurtech innovations are ineffective at enhancing organizations' cybersecurity, promoting the role of insurers as regulators, and helping insurers manage uncertainty. We conclude by offering recommendations on how society can help technology to assure algorithmic justice and greater security of consumer information as opposed to greater efficiency and profit.

INTRODUCTION

Artificial intelligence (AI),[1] predictive analytics,[2] and big data[3] are taking over society.[4] Governments, businesses, banks, advertisers, schools, healthcare, finance, and policing institutions all over the world are turning to emerging technologies and predictive analytics. The shift from an industrial economy focused on money, labor, and property as commodities to an economy focused on information is

[1] AI is commonly understood as a set of approaches and techniques deployed by computer scientists to assist computers in rationally addressing problems, regardless of the obstacles that they encounter. *See* NAT'L SCI. & TECH. COUNCIL, EXEC. OFFICE OF THE PRESIDENT, PREPARING FOR THE FUTURE OF ARTIFICIAL INTELLIGENCE 6–7 (2016). Although many of the techniques have been around for decades, computer scientists are now mobilizing these techniques because computers are faster and able to more easily absorb large amounts of unstructured information, commonly referred to as big data. *See* Randy Bean, *How Big Data Is Empowering AI and Machine Learning at Scale*, MIT SLOAN MGMT, REV. 2 (May 8, 2017), https://sloanreview.mit.edu/article/how-big-data-is-empowering-ai-and-machine-learning-at-scale/ [http://perma.cc/K4WP-WAVP] ("The availability of greater volumes and sources of data is, for the first time, enabling capabilities in AI and machine learning that remained dormant for decades due to lack of data availability, limited sample sizes, and an inability to analyze massive amounts of data in milliseconds."). We use the term "artificial intelligence" in this Article to include a broad array of computational techniques for predicting future outcomes based on analysis of past data. These techniques include "deep learning," "machine learning," and "learning algorithms," among others. While there are often important differences among these various types of AIs, these distinctions are not pertinent to the analysis in this Article.

[2] Predictive analytics refers to the use of statistical and analytical techniques to develop models that predict future events. *See* CHARLES NYCE, AM. INST. FOR CHARTERED PROP. CASUALTY UNDERWRITERS/INS. INST. OF AMERICA, PREDICTIVE ANALYTICS WHITE PAPER, 1 (2007). Predictions about what is likely going to occur are first generated by calculating how different qualities have been correlated with each other in the past and then using these correlations to make projections about what will happen in the future. Predictive analytics "almost exclusively refers to predictions that result from sophisticated technological analyses of large data sets. In commercial contexts, predictive analytics has been defined as the efforts of businesses to make sense of Big Data and gain insights that will provide competitive advantages over their peers." Max N. Helveston, *Consumer Protection in the Age of Big Data*, 93 WASH. U. L. REV. 859, 866 (2016).

[3] Big data are large, unstructured sets of data that are gathered from a variety of sources. This includes a variety of information from the internet and hard copies of documents from the physical world, including "online transactions, email, video, images, clickstream, logs, search queries, health records, and social networking interactions . . . sensors deployed in infrastructure such as communications networks, electric grids, global positioning satellites, roads and bridges, as well as in homes, clothing and mobile phones." Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 240 (2013). Big data are associated with having three defining qualities: "volume (the amount of data), velocity (the rate at which data is generated), and variety (the types of data collected)." Helveston, *supra* note 2, at 867.

[4] For a thorough exploration of the role of technology and data in society, see JULIE COHEN, BETWEEN TRUTH AND POWER (Oxford Univ. Press 2019).

reconstructing labor, money, and property as "datafied inputs to new algorithmic modes of profit extraction."[5] Data providers, harvesters, and refineries are paving the way for the "Fourth Industrial Revolution," one that extracts information from the available pool of consumers so that it may be reliably identified, analyzed, and used for profit.[6] Proponents of big data and emerging technology argue that these processes provide businesses with insights and perspectives on their customers, increase the efficiency of their operations, offer competitive advantages, and improve the use of existing products and services.[7] Opponents argue that corporate usage and exploitation of consumer information threaten privacy and data security.[8] Moreover, state and private-sector producers of surveillance technologies cultivate a global economic and social environment where very little is private.[9] It remains an open question whether the technological and big data revolution is transformative, disruptive, or harmful. The pivot toward technology in society, however, appears irreversible.

Although scholars are exploring the ways that code, technology, and information regulate society,[10] existing research—across many economic sectors

[5] *Id.* at 25.

[6] *See* KLAUS SCHWAB, THE FOURTH INDUSTRIAL REVOLUTION (Crown Bus. Publisher 2017) (highlighting the ramifications of technology on society). For a thorough history of the evolution into an economy based on information and data, see COHEN, *supra* note 4, at 20–55. Cohen describes the information capitalism process as one that involves data cultivation, data harvesting, data refineries, and ultimately data providers that market and sell this information to interested parties.

[7] *See* Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355 (2015) (highlighting the potential of big data); Tene & Polonetsky, *supra* note 3, at 243–44, 249–51 (2013) (discussing the business benefits of big data); ROB THOMAS & PATRICK MCSHARRY, BIG DATA REVOLUTION 141–43 (2015) (providing an overview of the benefits of big data).

[8] *See, e.g.*, Big Data and Consumer Privacy in the Internet Economy, 79 Fed. Reg. 32,714 (June 6, 2014); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 96–109 (2014) (discussing the use of predictive analytics and the privacy harms that occur); Benjamin Zhu, Note, *A Traditional Tort for a Modern Threat: Applying the Intrusion Upon Seclusion to Dataveillance Observations*, 89 N.Y.U. L. REV. 2381 (2014) (highlighting privacy and security problems).

[9] *See* COHEN, *supra* note 4, at 93 (discussing the rise of the surveillance-innovation complex, an environment where everyone is monitored at all times).

[10] For the economics and politics of enclosure and appropriation of informational resources, see generally JAMES BOYLE, SHAMANS, SOFTWARE, AND SPLEENS: LAW AND THE CONSTRUCTION OF THE INFORMATION SOCIETY (1996); James Boyle, *The Second Enclosure Movement and the Construction of the Public Domain*, 66 LAW & CONTEMP. PROBS. 33 (2003); Madhavi Sunder, *IP3*, 59 STAN. L. REV. 257 (2006). For a discussion of the ways that intellectual property law and policy structure global dynamics of development and resource distribution, see Anupam Chander & Madhavi Sunder, *The Romance of the Public Domain*, 92 CALIF. L. REV. 1331 (2004); Margaret Chon, *Intellectual Property and the Development Divide*, 27 CARDOZO L. REV. 2821 (2006). On how code is used as a regulatory

and aspects of society—primarily focuses on the theoretical and normative challenges of big data and emerging technologies.[11] Drawing upon legal, political, and economic theories, scholars offer normative arguments for and against big data, technology, and algorithmic governance in various contexts.[12] While theoretical and normative frameworks are helpful, much current scholarship lacks information on how these tools operate and what is actually happening on the ground.[13] This is not due to a lack of interest but rather the secrecy and lack of disclosure by data providers, data harvesters, and corporations that collect and use these data and operate these technologies.[14] Efforts by government and consumer advocacy organizations to access this information have failed.[15] Existing research in this area is not granular or nuanced enough to evaluate the impact of technology and data in society. To our knowledge, there has been very little empirical analysis of precisely *how* big data and technology influence important aspects of society. What are the processes and mechanisms through which big data and emerging technology influence society? Are these technologies harmful, disruptive, transformational, or a tool for corporate profit? Until we explore how big data, artificial intelligence, technology, and security operate on the ground in specific settings, the debate will remain frozen within normative arguments.

This Article offers one of the first deep-dive empirical examinations of how big data and emerging technologies shape and influence the delivery and practice of one particular industry that relies heavily on technology and big data: insurance. With among the lowest customer satisfaction and loyalty ratings of any industry,

instrument, see generally LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998). On the transformative potential of informational resources, see generally YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2006); BRETT M. FRISCHMANN, INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES (2012).

[11] For background on the theoretical and normative challenges of using technology and big data in the insurance context, see Rick Swedloff, *The New Regulatory Imperative for Insurance*, 61 B.C. L. REV. 2031, 2036 (2020).

[12] *See supra* note 10 and accompanying text.

[13] In addition, prevailing research on big data and technology focuses on the impact on individuals and ignores the way data are impacting businesses operating across many sectors.

[14] *See* COHEN, *supra* note 4, at 62 ("[T]he most noteworthy attribute of the personal data economy has been its secrecy, which frustrates the most basic efforts to understand how the internet search, social networking, and consumer finance industries sort and categorize individual consumers."); *see also* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 22–42, 64–80 (2015) (highlighting how the data processing practices of platform firms and data providers revolve around secrecy).

[15] *See* COHEN, *supra* note 4, at 62–63 (charting how the largest data providers continually stonewall and resist efforts by Congress and federal agencies to force greater disclosure of their information gathering practices).

insurance institutions have aggressively pivoted toward using technology and big data in the past ten years.[16]

The fusion between insurance and technology, commonly referred to as "insurtech," is revolutionizing the delivery of insurance.[17] In this Article, we focus on how insurers engage one of the most important threats to businesses and individuals in society: cybersecurity risks and data breach events.

Cyber risks are losses associated with the use of electronic equipment, computers, information technology, and virtual reality. These risks are crucial because consumer, financial, and health information is often stored in electronic form. Hackers, malware, social engineering, Internet of Things device attacks, and robocalls lead to identity theft, compromised personal, financial, and health information, and, in a small percentage of cases, physical damage as well. Breaches are pervasive and affect consumers and virtually every major industry.[18] Despite the proliferation of security and data breaches, consumer protection and privacy laws remain fragmented and have not significantly regulated the behavior of businesses that collect consumer data beyond requiring prompt notification of data breaches.[19]

Even though there are clear legal, reputational, and financial threats, existing research suggests that private organizations are not significantly changing their cybersecurity behavior. Despite having some cybersecurity measures in place, the

[16] *See* Samuel Lewis, *Insurtech: An Industry Ripe for Disruption*, 1 GEO. L. TECH. REV. 491, 491–492 (2017) ("[I]n 2014, investors poured $2.6 billion into 'insurtech,' over ten percent of all fintech investment that year and over a three-fold increase from the previous year.").

[17] *See id.*

[18] Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses*, 43 L. & SOC. INQUIRY 417, 418 (2018) [hereinafter Talesh, *Compliance Managers*] (outlining all the industries' cyberattacks and data breach events impact).

[19] In the United States, there is no single, comprehensive federal law regulating the collection and use of personal data. Instead, the United States operates with a variety of federal and state laws that sometimes overlap. Major federal laws that regulate privacy in different ways include, but are not limited to, the Federal Trade Commission Act, the Financial Services Modernization Act, the Health Insurance Portability and Accountability Act, the Fair Credit Reporting Act, and the Electronic Communications Privacy Act. In the United States, the Federal Trade Commission is attempting to try to regulate data security practices through its Unfair and Deceptive Acts and Practices statutes in commerce jurisdiction. The first law of its kind, the California Consumer Privacy Act, is a state-wide data privacy law that regulates how businesses all over the world are allowed to handle the personal information of California residents. The General Data Protection Regulation is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union. The highly fragmented nature of United States privacy and cybersecurity laws and regulations leaves most companies with no single standard with which to comply, creating confusion and frustration and weakening our overall national and economic security. For background on the fragmented regulatory structure over cybersecurity incidents, see COHEN, *supra* note 4, at 90–91,102–03; Talesh, *Compliance Managers*, *supra* note 18, at 418.

majority of organizations "do not believe they are sufficiently prepared for a data breach, have not devoted adequate money, training, and resources to protect consumers' electronic and paper-based information from data breaches, and fail to perform adequate risk assessments."[20]

Without strong and consistent legal regulations or adequate cybersecurity actions, insurance companies are stepping in and offering cyber insurance. This insurance provides first-party loss and third-party liability coverage for data breach events, cyberattacks, and privacy violations.[21] Insurers offering cyber insurance provide some risk shifting for the costs associated with having to respond to, investigate, defend, and mitigate against cyberattacks.[22] Although cyber insurance initially got off to a slow start, the cyber insurance industry is growing, with over $2 billion in total premiums annually.[23] Insurance companies now offer not only insurance but also risk management services aimed at improving organizations' cybersecurity profiles and reducing their risk.[24] In this respect, cyber insurers are playing a regulatory role over their insureds.

Technology and data have transformed the delivery of insurance in the cyber context because, unlike most traditional areas of insurance, cyber insurers lack significant amounts of loss history and actuarial data to rely on when making risk assessments.[25] Because cyber insurance is so new and uncertain—and the cyber risks and attacks from cyber attackers are constantly changing—cyber insurers covet data from data providers. Cyber insurers are turning to big data, AI, and predictive analytics to assist in the underwriting and risk and claims management processes and, as a result, are redefining the business of insurance.

Our empirical research for this project allows us to explore one of the most important issues currently debated among privacy and technology scholars: how big data, predictive analytics, and technology influence a particular industry in socially desirable or undesirable ways. We also simultaneously explore two questions that insurance scholars are currently wrestling with: how insurers manage uncertainty

[20] Talesh, *Compliance Managers, supra* note 18, at 419.

[21] *See* Shauhin A. Talesh, *Insurance Companies as Corporate Regulators: The Good, the Bad, and the Ugly,* 66 DEPAUL L. REV. 463, 475 (2017) [hereinafter Talesh, *Corporate Regulators*] (discussing the basic components of cyber insurance).

[22] *See id.*

[23] Trey Herr, *Cyber Insurance and Private Governance: The Enforcement Power of Markets*, 15 REGUL. & GOVERNANCE 98, 99 (2021) ("After relatively slow growth through the 1990s and 2000s, the size of the cyber insurance industry spiked upwards in 2012, from less than US$1 billion to more than US$2 billion in total premiums (as measured by the Betterley Report—an annual survey of the cybersecurity insurance market).").

[24] For a study on the way that insurers act as external compliance managers for businesses, see Talesh, *Compliance Managers*, *supra* note 18, at 425–35.

[25] *See infra* Section III.A and accompanying text. For further confirmation that insurers lack enough data to make proper risk evaluations, see Herr, *supra* note 23, at 99–102.

concerning underwriting risks using insurtech approaches[26] and how insurers use technology to regulate the behavior of businesses that purchase insurance.[27]

[26] *See generally* Tom Baker, *Uncertainty > Risk: Lessons for Legal Thought from the Insurance Runoff Market*, 62 B.C. L. REV. 59 (2021). Although many legal scholars think pricing and delivering insurance is a very predictable event, Baker notes that insurance in action is much more uncertain. Specifically, he notes that although insurance is thought of as a "fixed-in-advance distribution of determinable risks—in which insurance companies sell protection against defined categories of losses whose total costs can be accurately predicted and, therefore, priced with confidence when insurance is sold," the reality is "sociological research provides so many reasons why insurers so rarely hit that pricing nail on the head that legal scholars should stop thinking and acting as if insurers regularly could do so. Instead, we should start learning more about how insurers manage the uncertainty that the research reveals." *Id.* at 62, 66.

[27] For a comprehensive explanation of the concept of insurance as regulation, see generally Talesh, *Corporate Regulators, supra* note 21, at 469–74. The insurance as regulation debate has been a highly engaged area of legal scholarship over the last twenty years. Focusing on policy language, actuarial, and underwriting practices, many scholars argue that insurance covering product liability, workers' compensation, automobiles, homeowners, environmental liability, and tax liability regulate individuals and businesses in ways that are more constructive than government regulation. *See* Omri Ben-Shahar & Kyle D. Logue, *Outsourcing Regulation: How Insurance Reduces Moral Hazard*, 111 MICH. L. REV. 197, 217–28 (2012) (arguing insurers act as regulators often in favorable ways for society). Ben-Shahar and Logue note that because insurers have superior access to information and commercial sophistication, they use a series of techniques to improve the safety conduct of their policyholders. *Id.* at 231–38. Ben-Shahar and Logue conclude that because of insurers' inherent informational advantage, these institutions are better regulators than regulatory, legislative, or judicial institutions. *Id.* at 201. Other scholars have explored the relationship between insurance loss prevention and policyholder moral hazard across a variety of domains. *See generally* Shauhin Talesh, *Legal Intermediaries: How Insurance Companies Construct the Meaning of Compliance with Antidiscrimination Laws*, 37 L. & POL'Y 209, 212–14 (2015) (examining employment discrimination); Talesh, *Compliance Managers*, *supra* note 18, at 417 (examining cybersecurity); George M. Cohen, *Legal Malpractice Insurance and Loss Prevention: A Comparative Analysis of Economic Institutions*, 4 CONN. INS. L.J. 305 (1997) (examining legal malpractice); Anthony E. Davis, *Professional Liability Insurers as Regulators of Law Practice*, 65 FORDHAM L. REV. 209 (1996) (examining legal malpractice); Katherine Baicker & Amitabh Chandra, *The Effect of Malpractice Liability on the Delivery of Health Care*, NAT'L BUREAU ECON. RSCH. (Aug. 2004), https://www.nber.org/papers/w10709 [https://perma.cc/KZT4-VDVF] (examining medical malpractice); Tom Baker, *Medical Malpractice and the Insurance Underwriting Cycle*, 54 DEPAUL L. REV. 393 (2005) (examining medical malpractice); Bernard Black, Charles Silver, David A. Hyman & William M. Sage, *Stability, Not Crisis: Medical Malpractice Claim Outcomes in Texas, 1988–2002*, 2 J. EMPIRICAL LEGAL STUD. 207 (2005) (examining medical malpractice); Elizabeth O. Hubbart, *When Worlds Collide: The Intersection of Insurance and Motion Pictures*, 3 CONN. INS. L.J. 267, 267 (1996) (examining motion picture industry); Tom Baker & Thomas O. Farrish, *Liability Insurance and the Regulation of Firearms*, SUING THE GUN INDUSTRY: A BATTLE AT THE CROSSROADS OF GUN CONTROL AND MASS TORTS 292, 292 (Timothy D. Lytton ed., 2005) (examining firearms);

Drawing from sixty interviews from members of the cyber insurance field, a quantitative analysis of a "big data" set we obtained from a cyber insurance data provider, and observations from cyber insurance conferences—and by evaluating and coding cyber insurance company applications—we identify and explore the effects and implications of what we refer to as the "technologization of insurance," the process whereby technology influences and shapes the delivery of insurance. In doing so, we reveal how technology, data, and security are mechanisms through which insurers attempt to manage uncertain cyber risks and regulate the behavior of their policyholders.[28]

We present our findings in two phases. Part I explores how technology actually shapes the delivery of insurance. We find that, among brokers and insurers, and at every stage of the insurance cycle, insurtech is transforming the delivery of insurance. Insurance brokers and underwriters rely on technology to assess the risk of the prospective insured. Technology, predictive analytics, and security surveillance supplant the traditional insurance application and interview process.[29] Brokers and insurers also use big data to compile information about past losses and breaches of similar companies to develop benchmarks, predict the risk of companies seeking insurance, and price appropriate premiums.[30] Insurers, themselves or in partnerships with information security companies, rely on technology to offer pre-breach services to insureds, hoping to detect and prevent cybersecurity attacks.[31]

Part II highlights the effects and implications of the technologization of insurance. Although reliance on technology and data are increasingly transforming the way insurers advertise, underwrite, and price insurance, the actual impact on insurer behavior seems to have remained minimal and is largely symbolic. We find that insurtech interventions and innovations have been, to date, largely ineffective at enhancing organizations' cybersecurity and assisting insurers in managing uncertainty in the market.[32] Even utilizing big data and technology, insurers, by and large, are not requiring organizations to improve their cybersecurity health prior to offering insurance. Surprisingly, our empirical findings also indicate that most insurers do not even offer significant premium discounts for specific cybersecurity improvements.[33]

Regarding the pre-breach risk management services that insurers tout, which rely on surveillance and security technologies to prevent insureds from being

STEPHEN D. SUGARMAN, DOING AWAY WITH PERSONAL INJURY LAW: NEW COMPENSATION MECHANISMS FOR VICTIMS, CONSUMERS, AND BUSINESS (1989) (examining personal injury); John Rappaport, *How Private Insurers Regulate Public Police*, 130 HARV. L. REV. 1539, 1539 (2017) (examining policing practices).

[28] To be clear, we are not suggesting that all insurers rely heavily on technology, but rather, based on our research, those that do rely on it in the cyber insurance field, use it in these ways.

[29] *See infra* Part III.

[30] *See id.*

[31] *See id.*

[32] *See infra* Part IV.

[33] *See id.*

breached, our interviews reveal that very few insureds actually use these services, rendering these risk management interventions and insurers' role as regulators over its insureds ineffective.[34] In contrast to the narrative that big data can produce greater efficiency and more precise pricing and risk predictions for insurers, our analysis of a big data database that we purchased reveals that big data in the cyber context is an unreliable tool that is often manipulated by the insurance industry and used to nudge buyers toward purchasing more insurance.[35] Instead of providing a more complete and precise picture of cyber events and risks, the data provides a biased view that is manipulated to the detriment of consumers. Although cyber insurers are turning to big data and technology as mechanisms to understand risk, such models often are not fully integrated into the underwriting and risk management processes.

Further, our findings underscore a crucial point: big data, AI, and emerging technologies are not all the same. Data scientists and programmers have multiple opportunities to shape their development.[36] Our empirical research reveals that emerging technologies are not neutral but are configured and constructed in subtle ways by individuals and organizations that develop these technologies. Thus, the issue is not whether data and technology are good or bad or effective or ineffective but rather under what conditions do these technologies lead to socially desirable or undesirable outcomes. Our insights come from within the corporate world and reveal how the technologization of insurance is mobilized and leads to unneutral outcomes that further the insurance industry but do not necessarily make businesses and individuals (and, therefore, society) more cyber-secure.

While most empirical research projects end with an analysis and implications of their findings, this Article also offers a pathway forward explaining how insurtech might work more effectively for insurers, businesses, and consumers. We offer a series of recommendations on how the private sector can help weaponize technology for greater safety and security of consumer information, as opposed to using it solely for capitalism, profit, and efficiency.[37] Despite the problems with the insurtech model that we uncovered, our research also suggests that a new model of insurance that incorporates some of the best tools of a fully integrated technology and insurance model, anchored around continuous or "real-time" underwriting, risk management, and risk-based pricing that rewards organizations for enhanced cybersecurity, may be effective.[38] We focus on two examples that incorporate these approaches. We argue that the fully integrated insurtech approaches offer at least a window into a new approach for the delivery of insurance that state regulators should

[34] *See id.*

[35] *See id.*

[36] *See* COHEN, *supra* note 4, at 3 ("Scholarship in science and technology studies has shown that new technologies do not have predetermined, neutral trajectories, but rather evolve in ways that reflect the particular, situated values and priorities of both their developers and their users.").

[37] *See infra* Part V.

[38] *See id.*

evaluate.[39] We also offer some recommendations on how the federal government can help insurtech work in ways that enhance the security and safety of consumer information.

Part I of this Article explores how big data and emerging technologies influence the insurance industry, including early forms of insurtech partnerships.[40] After briefly highlighting our methodology in Part II,[41] Part III explores, for the first time, how technology is influencing insurance underwriting and risk and claims management processes.[42] Part IV examines the implications and effects of the technologization of insurance.[43] Finally, Part V offers some recommendations that could improve the use of insurtech approaches in the insurance industry and foster greater algorithmic justice.[44]

I. BIG DATA AND ARTIFICIAL INTELLIGENCE'S INVOLVEMENT IN INSURANCE

Part I briefly highlights the history of insurtech, the role of big data, AI, and technology in insurance; the pros and cons of using emerging technologies in insurance; and state and federal attempts to regulate the expansion of insurtech. This information lays the foundation for understanding the implications of our empirical study of insurtech that follows.

A. Insurance: The Basics

Although there is not one formal definition of what insurance is, the function of insurance is to protect the policyholder in the event of a future loss and provide a formal mechanism for sharing the costs for misfortune or injurious experiences.[45] Contemporary insurance arrangements are designed around a formal, organized scheme for the distribution of an economic loss over a large number of persons subject to the risk of a particular loss, with a goal of replacing the uncertain risk of loss with a predictable cost.[46] The loss is often distributed by transferring the risk to an insurer.[47] The loss is distributed in advance, often by charging a fixed premium

[39] *See id.*

[40] *See infra* Part I.

[41] *See infra* Part II.

[42] *See infra* Part III.

[43] *See infra* Part IV.

[44] *See infra* Part V.

[45] For a thorough background on the fundamentals of insurance, see KENNETH ABRAHAM, INSURANCE LAW AND REGULATION: CASES AND MATERIALS 3–5 (5th ed. 2010) [hereinafter ABRAHAM, INSURANCE LAW]. *See generally* KENNETH ABRAHAM, DISTRIBUTING RISK: INSURANCE, LEGAL THEORY, AND PUBLIC POLICY 1–20 (1986) (explaining the concepts of risk and insurance).

[46] ABRAHAM, INSURANCE LAW, *supra* note 45, at 3–4.

[47] *Id.*

or an assessment or deductible after the event, or by some combination of these.[48] The premium amount is determined through underwriting, a systematic process of measuring risks and assigning dollar amounts to them. A premium varies based on how likely a person is to experience an adverse effect as compared to the average insured party. To manage the uncertainty of issuing insurance, underwriters collect information from applicants for insurance, including answers to insurance applications, interviews, actuarial data, and loss control evaluations. Once the insurance policy is issued, insurers pay for covered losses under the policy up to the agreed-upon policy limits.[49]

B. Insurtech: Background and History

Short for insurance technology and labeled a "disrupter,"[50] insurtech is the innovative use of technology in insurance, big data, cloud infrastructure, blockchain, and peer-to-peer, usage-based, and on-demand insurance.[51] Insurtech is useful for collecting and analyzing data to provide better service to insureds, especially since insureds expect constantly improving experiences with any company they interact with. While the use of data is not new to the insurance industry, technological advances have made more data available that can be used to enhance or replace traditional functions in the industry, namely back-office systems, risk assessment, underwriting, fraud detection, and claims processing.[52] This affects how insurance is distributed and, in theory, reduces costs for both the insurer and insured.

Lemonade, Inc. is considered an insurtech pioneer in the United States. Founded in 2016, Lemonade focuses on peer-to-peer ("P2P") online property and

[48] *How Does Insurance Work?*, ASS'N BRIT. INSURERS (Nov. 13, 2014), https://www.abi.org.uk/Insurance-and-savings/Tools-and-resources/How-insurance-works [http://perma.cc/LM2H-U42Z].

[49] ABRAHAM, INSURANCE LAW, *supra* note 45, at 4 ("By pooling uncorrelated risks the insurer takes advantage of the law of large numbers and turns a large number of individually risky undertakings into a highly predictable set of obligations."). We note that once the policy limits are exhausted, the insurance company's obligations to indemnify an insured end.

[50] Angela Ziegler Roschmann, *Digital Insurance Brokers—Old Wine in New Bottles? How Digital Brokers Create Value*, 107 ZVERSWISS 273, 275 (2018) (noting that insurtech has the potential to cause disruptive change to the industry).

[51] For a thorough background on insurtech, see U.S. DEP'T OF THE TREASURY, FEDERAL INSURANCE OFFICE, ANNUAL REPORT ON THE INSURANCE INDUSTRY 61 (2018), https://www.treasury.gov/initiatives/fio/reports-and-notices/Documents/2018_FIO_Annual_Report.pdf?57 [https://perma.cc/87VF-FPXG].

[52] Bridget Hagan, *Big Data, Big Questions—Insurers and Advanced Data Analytics*, 21 NO. 1 FINTECH L. REP. NL 2 (2018) (describing the various interventions and interactions between insurance and technology). Indeed, insurtech spans across the entire insurance value chain and all lines of insurance. Startups are "reaching customers through new distribution mediums—addressing shifts in the way people communicate, access information and make decisions—while not disturbing traditional channels." *Insurtech*, NAT'L ASS'N INS. COMM'RS, https://content.naic.org/cipr_topics/topic_insurtech.htm [https://perma.cc/SRD3-ZA6X] (last updated Feb. 19, 2020).

casualty insurance.[53] Licensed as an insurer, Lemonade digitized the entire insurance process, replacing brokers and paperwork with algorithms and allowing insureds to purchase insurance through mobile apps or via its website in minutes.[54] Its user-friendly interface helps insureds interact with two chatbots that simplify both the enrollment and claims settlement process.[55]

Lemonade uses a nontraditional premium structure. Whereas traditional insurance companies keep the money that is not paid out in claims, Lemonade's insureds "pay a certain premium which includes a fixed fee kept by the company. The rest is used to pay claims. Anything leftover is then donated to a charity . . . ."[56] This feature is known as "Giveback," and the charities are nominated by the insureds.[57] Insureds are pooled together by the charities they choose, thus pairing insureds with similar interests.[58] It also helps to protect against fraudulent claims by having insureds pool their premiums and entice them to have more left in the pool to donate to charities. Lemonade states that its "20 percent cut of premiums is well below other insurers' cost ratios, which stand at about 35 percent."[59] Lemonade believes it will donate more to charities than it takes in profit,[60] making this Giveback promise one reason why it is favored among insureds.[61] Furthermore, Lemonade's automated environment allows insureds to make real-time alterations to provisions such as deductibles or limits without involving a customer service

[53] *See Peer-to-Peer Personal Lines Insurer Lemonade Opens for Business in New York*, INS. J. (Sept. 21, 2016) https://www.insurancejournal.com/news/east/2016/09/21/427092.htm [https://perma.cc/6JVA-VVQB].

[54] *See* Lewis, *supra* note 16, at 500–01 (2017) (explaining how Lemonade operates).

[55] *See id.*

[56] *Id.* at 501.

[57] *About Lemonade*, LEMONADE, http://www.lemonade.com/faq#service [https://perma.cc/GN96-AM7H] (last visited June 13, 2021); Oliver Ralph, *Lemonade Aims to Shake Up Insurance with Charity Promise*, FIN. TIMES (Sept. 21, 2016), https://www.ft.com/content/477bff26-7f23-11e6-bc52-0c7211ef3198 [https://perma.cc/TW8S-THCB]; *see also* Lewis, *supra* note 16, at 501.

[58] *See* Ralph, *supra* note 57.

[59] *Id.*

[60] *Id.* In fact, Lemonade reported that through Giveback, it had donated $631,540 in 2019 to charities such as the ACLU, The Trevor Project, charity: water, Teach for America, UNICEF, American Red Cross, and more. *How to Make a Dent in the Universe with the Lemonade Giveback*, LEMONADE: BLOG, (Mar. 28, 2019), https://www.lemonade.com/blog/social-impact-meets-insurance/#impact [https://perma.cc/9PVX-HHCX]. This impact includes supporting "224,000 low-income students through Teach for America, distributing 42,589 packets of food to malnourished children with UNICEF, funding five water projects with charity: water—bringing safe, clean drinking water to thousands of people, funding suicide prevention support for 1,683 LGBTQ+ youth via The Trevor Project, and helping fund the ACLU's fight in court to reunite immigrant families." *Id. See Giveback 2019*, LEMONADE, https://www.lemonade.com/giveback-2019 [https://perma.cc/9AW9-YTSQ] (last visited July 20, 2021) for further examples of its impact in 2019.

[61] Roschmann, *supra* note 50, at 283.

representative.[62] Originating in New York, Lemonade now also offers coverage in thirty-six other states and the District of Colombia and is looking to expand.[63]

Insurtech activity is significantly increasing across the insurance industry, attracting $16.5 billion in investments over the past decade.[64] Some insurers use on-demand insurance platforms that allow customers to enroll or disenroll whenever they want—they do not have to commit to an annual policy as required by traditional insurance companies.[65] Insurtech approaches also include insurance apps that allow consumers to purchase coverage through their smartphones and use AI to analyze trends and improve risk modeling. While many of these technologies were pioneered by technology startups, some established insurance companies are incorporating these new technologies into their business practices through innovative methods.[66]

[62] Susanne Sclafane, *Insurtech Lemonade Opens Its Sales Platform for All to Use*, INS. J. (Oct. 12, 2017), https://www.insurancejournal.com/news/national/2017/10/12/467209.htm [https://perma.cc/QK38-YCK3].

[63] *See About Lemonade*, *supra* note 57.

[64] *Insurtech*, NAT'L ASS'N INS. COMM'RS, *supra* note 52 (citing DELOITTE, ACCELERATING INSURANCE INNOVATION IN THE AGE OF INSURTECH 6 (2019), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-accelerating-insurance-innovation.pdf [https://perma.cc/HMQ6-75GQ]).

[65] Andrea Wells, *Insurance Tries to Keep Up with Sharing Economy*, INS. J. (Feb. 4, 2019), https://www.insurancejournal.com/news/national/2019/02/04/516652.htm [https://perma.cc/U8SW-P49K]. *See also* Mark Hollmer, *Slice Labs Testing Pay-Per-Use Insurance App with Rideshare Drivers*, INS. J. (Apr. 3, 2017), https://www.insurancejournal.com/news/national/2017/04/03/446575.htm [https://perma.cc/6TUW-HPQP] (describing Slice Lab's "pay-per-use" insurance model that allows customers to enroll or disenroll whenever they want).

[66] *See* Greg Tourial, *State Regulators Discuss New Technologies at Insurtech Conference*, 2018 WL 4783738 (2018) (highlighting the insurance industry's increased pull toward incorporating predictive analytics and emerging technologies into its model). For a thorough explanation of how insurers are integrating technology into their own insurance platforms, see *Nationwide Launches New Digital Insurance Product on Socotra*, GLOBENEWSWIRE (Dec. 11, 2019), https://www.globenewswire.com/news-release/2019/12/11/1959181/0/en/Nationwide-launches-new-digital-insurance-product-on-Socotra.html [https://perma.cc/33DD-5PU8]. Recently Nationwide Mutual Insurance Company, one of the largest insurances and financial services organizations in the United States, launched its new digital insurance platform: Spire. Relying on a core operating system called Socotra, which "unifies underwriting, policy management, claims, reinsurance, reporting, and more," Spire allows potential insureds to secure auto insurance coverage using a mobile device "by simply scanning a driver's license and answering four questions about driving behavior. The entire process takes less than a minute and does not require the customer to engage with an agent. Spire also ensures that customers' premiums are based on logical, transparent factors (such as age, payment history, and where and how they drive)" and uses layman's terms. *Id.*

C. The Engine Behind Insurtech: Big Data

Big data have no single definition[67] but generally refer to a complex volume of data and a set of technologies that analyze and manage it.[68] This abundance of information is created by daily activities and collected by all types of commercial and governmental entities from both online and offline sources and devices.[69] Big data are analyzed through data mining, statistical modeling, and machine learning to identify patterns, categorize new occurrences, and make predictions (i.e., predictive analytics).[70] These predictions are used to enhance practices such as in operations or marketing.[71] Algorithms drive the analytics.[72] Compared to regular data, big data require the use of technologies that can analyze data that are not stored in a uniform format, not centrally located, and incomplete.[73] Big data are too complex for traditional processing techniques.

Data are fundamental to insurance. Though the industry was slow to adopt insurtech innovations, throughout the 2000s, insurers expanded their use of big data analytics and started using data from social networks and other third-party sources rather than solely asking for information directly from insureds.[74] For example, in the property and casualty insurance industry, policies were historically priced based on fewer than twenty variables and were fine-tuned with a standard list of questions.

[67] Robert D. Helfand, *Big Data and Insurance: What Lawyers Need to Know and Understand*, 21 J. INTERNET L. 1, 3 (2017) (noting the multifaceted ways to define big data).

[68] *Id.* at 6; *Big Data*, NAT'L ASS'N. OF INS. COMM'RS, https://content.naic.org/cipr_topics/topic_big_data.htm [https://perma.cc/Y672-7VBA] (last updated Mar. 27, 2020).

[69] Helveston, *supra* note 2, at 868–69; Rick Swedloff, *Risk Classification's Big Data (R)evolution*, 21 CONN. INS. L.J. 339, 353 (2014). Specifically, online sources include "transactions, email, video, images, clickstream, logs, search queries, health records, and social networking interactions." Tene & Polonetsky, *supra* note 3, at 240. Offline records include public records (e.g., criminal records, deeds, corporate filings), retailers' sales records, credit agencies reports, etc. Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 404–05 (2014). Additionally, devices include cell phones, surveillance cameras, global positioning satellites, utility-related sensors, communication networks, phonebooths, etc. EXECUTIVE OFFICE OF THE PRESIDENT, THE WHITE HOUSE, REPORT TO THE PRESIDENT—BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 22–24 (2014). See Helfand, *supra* note 67, at 3–6, for more specific examples.

[70] Helveston, *supra* note 2, at 870–71 (highlighting the various approaches to big data).

[71] *See id.*

[72] An algorithm is a set of instructions for solving a problem or accomplishing a task. Every computerized device uses algorithms to perform its functions. Algorithms often reduce the time it takes to accomplish tasks manually. Models and predictive analytics are reliant on algorithms. For background on algorithms, see Lucas Downey, *Algorithm*, INVESTOPEDIA (Oct. 29, 2019), https://www.investopedia.com/terms/a/algorithm.asp [https://perma.cc/6NSE-UTBF].

[73] *See* Helveston, *supra* note 2, at 867.

[74] Michael W. Elliot, *Big Data Analytics: Changing the Calculus of Insurance*, CIPR NEWSLETTER 20 (2017), https://www.naic.org/cipr_newsletter_archive/vol23_big_data.pdf [https://perma.cc/KS6C-6KEF] (noting the significant increase among insurers using big data).

Now, insurers use additional data from new and nontraditional sources, with more than 1,000 variables and granular rating classes.[75] In fact, digital broker Acxiom says it has intelligence on 700 million individuals,[76] which could—among other things—reveal "3,000 propensities for nearly every US consumer[.]"[77] Another digital broker, TowerData, offers "demographic, interest and purchase data on 80% of [U.S.] email or postal addresses."[78]

Yet, while insurers have always analyzed information to make underwriting decisions, big data have transformed how data scientists analyze information. Traditionally, the goal of insurance analysis is to quantify information and "'average away' the noise of individuals"—anything "contingent, accidental, inexplicable, or personal"—so that an individual becomes part of a homogenous group, and the group forecasts the value of the risk an individual may have.[79]

However, big data reversed this perspective. Real-time data are now seen as more trustworthy than static parameters such as insurance applications.[80] As opposed to understanding movements and regularities on the aggregate, predictive analytics focus on the individual.[81] Big data leads data scientists to look "at each

[75] Hagan, *supra* note 52, at 1; Alex Woodie, *How Big Data Is Shaking Up the Insurance Business*, DATANAMI (Jan. 5, 2016), https://www.datanami.com/2016/01/05/how-big-data-analytics-is-shaking-up-the-insurance-business [https://perma.cc/B7T5-28Y2]. Over the past two decades, insurers have increasingly begun to deploy data from third-party data sources. For example, when empirical evidence emerged that people with higher credit scores also tend to be safer drivers, insurers started to incorporate credit scores into their analysis for personal auto insurance. Richard Clarke & Ari Libarikian, *Unleashing the Value of Advanced Analytics in Insurance*, MCKINSEY & CO. (Aug. 1, 2014), https://www.mckinsey.com/industries/financial-services/our-insights/unleashing-the-value-of-advanced-analytics-in-insurance [https://perma.cc/K674-V4N6].

[76] ACXIOM CORPORATION, 2018 ANNUAL REPORT 12 (2018), https://www.annualreports.com/HostedData/AnnualReports/PDF/NASDAQ_ACXM_2018.pdf [https://perma.cc/K674-V4N6].

[77] ACXIOM CORPORATION, 2014 ANNUAL REPORT 8 (2014), https://www.annualreports.com/HostedData/AnnualReportArchive/a/NASDAQ_ACXM_2014.pdf [https://perma.cc/J57J-CHQT].

[78] *Email-Intelligence*, TOWERDATA, INC., http://www.towerdata.com/email-intelligence/email-enhancement [https://perma.cc/7N6D-YVVK] (last visited July 30, 2020).

[79] Laurence Barry & Arthur Carpentier, *Personalization as a Promise: Can Big Data Change the Practice of Insurance?*, 7 BIG DATA & SOC'Y 1, 3–4 (2020) (quoting THEODORE M. PORTER, TRUST IN NUMBERS 85 (1996)).

[80] *Id.* at 5 (noting questionnaires are now an "obsolete, cumbersome, and inaccurate process for data collection" and real-time data are "perceived as more trustworthy than demographic, static parameters").

[81] *Id.* at 5–6 ("Whereas forecasting estimates *the total number of ice cream cones* to be purchased next month . . . , predictive analytics tells you *which individual[s] . . . are most likely to be seen* with a cone in hand.") (quoting ERIC SIEGAL, PREDICTIVE ANALYTICS: THE POWER TO PREDICT WHO WILL CLICK, BUY, LIE, OR DIE 16 (2013)) (emphasis in original).

individual in their irreducible differences, rather than discarding them, and assessing their risk as if each individual were their own class."[82]

Consequently, big data are integrated into marketing, underwriting, claims handling, and risk management—practically every aspect of insurers' operations.[83] Insurtech companies and large insurers across health, life, property, and casualty insurance aggressively pursue ways to incorporate big data into their operations.[84] In fact, the insurance industry invests $2.4 billion in big data technologies, and these investments are expected to increase to $3.6 billion in 2021.[85] A 2017 survey revealed that 51 percent of insurers surveyed use big data analytics for claims modeling in efforts to reduce claims, and 42 percent use analytics for actuarial model testing and underwriting.[86] These numbers are increasing rapidly as technology advances and insurers realize the benefits of its use.

[82] *Id.* at 6 (emphasis in original). Big data traces even the merest "breadcrumbs" of data. *Id.* (quoting ALEX PENTLAND, SOCIAL PHYSICS: HOW GOOD IDEAS SPREAD—THE LESSONS FROM A NEW SCIENCE 8 (2014)).

[83] *Id. See, e.g.*, PETER CORBETT, MICHAEL SCHROEK & REBECCA SCHOCKLEY, IBM INST. FOR BUS. VALUE, ANALYTICS: THE REAL-WORLD USE OF BIG DATA IN INSURANCE 3–7 (2013) (describing how advanced analytics could be incorporated into insurers' marketing, underwriting, claims management, and other practices).

[84] BENNO KELLER, THE GENEVA ASSOCIATION, BIG DATA AND INSURANCE: IMPLICATIONS FOR INNOVATION, COMPETITION, AND PRIVACY 9 (2018) (noting that big data has "triggered an arms race in the development of new applications along the entire insurance value chain, both by InsurTech startups and established insurers").

[85] *See Insurtech*, NAT'L ASS'N. OF INS. COMM'RS, *supra* note 52 (highlighting the prevalence of big data among insurers); Alex Gayduk, *How Big Data Impacts the Insurance Industry and Beyond*, YES MAGAZINE (July 24, 2019), https://yfsmagazine.com/2019/07/24/how-big-data-impacts-the-insurance-industry-and-beyond [https://perma.cc/8GJR-9AQC] ("The adoption of big data is constantly increasing, and insurance companies are expected to invest in these technologies up to $3.6 billion by 2021."); Mae Rice, *21 Big Data Insurance Companies to Know*, BUILT IN, https://builtin.com/big-data/big-data-insurance [https://perma.cc/HK8K-XHCG] (last updated Apr. 6, 2020) (highlighting twenty-one insurance companies and how they are leveraging big data).

[86] Lou Brothers, Carrie Camino, Greg Layok & Brad Ptasienski, *Survey Finds Insurers Not Fully Realizing Benefits*, NU PROP. CASUALTY 360 (Mar. 20, 2017, 2:00 AM), http://www.propertycasualty360.com/2017/03/20/survey-finds-insurers-not-fully-realizing-benefits [https://perma.cc/L57U-UJCG]. With underwriting, big data "offers insurers technologies that can enhance the scope and accuracy of their predictive models and provides them with cheap access to an abundance of information about individuals, the two prerequisites for identifying qualities that correlate with risk of loss in a cost-effective manner." Helveston, *supra* note 2, at 879. *See* CORBETT ET AL., *supra* note 83, at 6 (describing how new technologies enabled an auto insurer to collect better data on its customers and identify factors that correlate with risk); NYCE, *supra* note 2, at 5–7 (describing how predictive analytics can improve insurers' ability to detect risk factors).

D. Pros of Emerging Technologies and Big Data for the Insurance Industry

Insurers argue that emerging technologies and big data improve profits, raise customer satisfaction, and lower administrative costs.[87] One industry analyst indicated these techniques have resulted in 30 percent better access to insurance services, 40–70 percent cost savings in claims processing and management, 60 percent higher fraud detection rates, 90 percent faster nonemergency claims processing, and 50 percent reduction in administrative workload.[88]

Advocates for insurtech argue that big data and technology improve the speed and efficiency in all stages of the insurance cycle, from marketing to underwriting to loss prevention to claims management. The traditional insurance model requires manual entry of data and approvals among multiple people in the insurance company.[89] With the availability of big data and technological advancements, insurers can now use inexpensive methods to collect large amounts of information and process claims.[90]

Insurtech also allows for personalization in underwriting practices—and thus price optimization—rather than simply identifying an individual within risk pools and assigning them a price that accounts for the pool but not the individual. Rather than assessing risk by age, zip code, and past accident record, big data enables insurers to expand the types of information that factor into their rate-setting and underwriting practices.[91] In theory, these independent variables have the potential power to predict losses.[92] In some cases, insureds could pay lower premiums otherwise unavailable to them.[93] Some argue that charging everyone rates that

[87] Tanguy Catlin, Johannes-Tobias Lorenz, Christopher Morrison & Holger Wilms, *Time for Insurance Companies to Face Digital Reality*, MCKINSEY & COMPANY (Mar. 9, 2017), https://www.mckinsey.com/industries/financial-services/our-insights/time-for-insurance-companies-to-face-digital-reality# [https://perma.cc/TX2J-BJGL] (highlighting the need to transform the way insurance companies operate).

[88] Gayduk, *supra* note 85 (providing data on the way technology and big data influence the insurance industry).

[89] *See* ROB THOMAS & PATRICK MCSHARRY, BIG DATA REVOLUTION: WHAT FARMERS, DOCTORS AND INSURANCE AGENTS TEACH US ABOUT DISCOVERING BIG DATA PATTERNS 51–56 (Wiley, 2015) (noting that big data and technology have moved the insurance process from eight weeks to eight days).

[90] *See* Helveston, *supra* note 2, at 882–83. As such, using big data to assess insureds' risk profile can be cost-effective for both the insurer and the insured. Rather than use "prohibitively large amounts of labor" to comb through and to combine various sources that could affect the risk profile or provide indirect evidence of fraudulent behavior, insurers can use big data and thus "inexpensive computer processing power and storage" to automate the process with little human oversight. *Id.*

[91] Catlin et al., *supra* note 87.

[92] Swedloff, *supra* note 11, at 2057 (noting "independent variables presumably [have] the power to predict loss" in the insurtech context).

[93] *InsurTech: Where Are We Now?*, NORTON ROSE FULBRIGHT (Feb. 2017), https://www.nortonrosefulbright.com/en/knowledge/publications/db154724/insurtech-

reflect each person's individual risk is more actuarially fair than a system that forces some individuals to subsidize others.[94] Technology and data can also be used to more readily detect and prevent claims fraud, benefiting both insurers and the insured.[95]

Finally, emerging technologies and big data offer insurers the ability to engage in loss prevention and risk mitigation. For example, the use of wearable devices and telematics in automobile insurance allows for higher-level risk mitigation because these devices can identify warning signs and alert insurers of potential issues long before insurers identify them. [96] This technology allows for real-time, rapid responses and automation and leads the industry to "move from reacting to losses to

where-are-we-now [https://perma.cc/TX2J-BJGL] (arguing that a more fine-tuned risk profile leads to reduced premiums).

[94] "This boost in predictive power, paired with continued automation of the underwriting process, will increase insurers' ability to tailor policy rates on a policyholder-by-policyholder basis. Once this occurs, insurance markets will begin to exhibit an unprecedented level of actuarial fairness." Helveston, *supra* note 2, at 884. Insurers will be able to identify both better and worse risks and price these different risks correctly. Indeed, a system that "charges everyone rates that reflect each individual's level of risk" may be "more fair than a system that forces some individuals to subsidize others." *Id.* at 885; s*ee, e.g.*, Swedloff, *supra* note 11, at 346 ("[P]ricing based on risk may be more fair to low risk insureds."); Tom Baker, *Containing the Promise of Insurance: Adverse Selection and Risk Classification*, 9 CONN. INS. L.J. 371, 383 (2003) ("The leading moral justifications for risk classification are the following: 1) without risk classification, low risks are unfairly forced to subsidize high risks.").

[95] By basing "appraisals on 'an in-depth assessment of the person or business in question' and 'their connections to other people, businesses, groups, vehicles, properties etc.,'" machine learning can discern connections between the various factors that may be imperceptible to human eyes or are not intuitive. It can then use AI and data sets to learn and improve from experience, with no extra programming. The continuous revision and application of variations in data analysis allows the AI to anticipate the discovery of new fraud schemes. Helfand, *supra* note 67, at 11 (quoting QBE INSURANCE GROUP LIMITED, INNOVATIONS IN USING SOCIAL MEDIA TO FIGHT INSURANCE FRAUD, IMPROVE SERVICE (2016)).

[96] Lewis, *supra* note 16, at 494–495; *see generally* Alison Coleman*, Four Insurtech Startups Shaking Up the Insurance Industry*, FORBES (July 9, 2019, 8:24 AM EDT), https://www.forbes.com/sites/alisoncoleman/2019/07/09/four-insurtech-startups-shaking-up-the-insurance-industry/#2d8a0aed29f4 [https://perma.cc/L92C-8FCU] (providing the example of Tractable, which can apply "AI to accident and disaster recovery" to "look[ ] at the asset damage and predict[] repair costs from photos in real-time, so that claims can be settled faster").

preventing losses," from insuring against risk to insuring prevention.[97] Proactive risk management, in theory, can reduce unexpected premium increases.[98]

E. Cons of Emerging Technologies and Big Data for the Insurance Industry

Despite the positive outcomes that insurtech may bring, its use may also result in negative consequences. For starters, there are concerns with the quality and reliability of big data. Though big data can be useful to find correlations, errors can exist in the data themselves, especially if they come from unreliable sources that are likely to suffer outages and other losses or when data harvesters merge multiple data sets together.[99] Indeed, big data can still be wrought with errors due to selection bias, inaccuracy, or subjective judgment even when the information itself is accurate.[100] Even if the data are clean and unbiased, algorithms could mistakenly find correlations with statistical significance that have no meaningful connection between the variables.[101]

Big data also raise privacy concerns. Data can be obtained and harvested without knowledge or consent of those whose information is being collected.[102] Although big data are typically not used to identify specific individuals, there is no

[97] Elizabeth Blosfield, *Imagining How Technology Might Transform Risks and Insurance by 2030*, INS. J. (Nov. 7, 2019), https://www.insurancejournal.com/news/national/2019/11/07/547850.htm [https://perma.cc/5M3U-YY22]; *see* Catlin et al., *supra* note 87 (highlighting how insureds "pay not for premiums in order to be compensated for damages they might incur, but for gadgets or services that predict and help prevent that risk"); Jemima Kelly & Carolyn Cohn, *Insurers Hope Insurtech Will 'Nudge' Customers to Less Risky Behaviors*, INS. J. (Sept. 19, 2017), https://www.insurancejournal.com/news/national/2017/09/19/464718.html [https://perma.cc/ZCZ4-5S9L].

[98] *Friendsurance: Friends with Benefits?*, HAR. BUS. SCH. DIGIT. INITIATIVE (Mar. 26, 2018), https://digital.hbs.edu/platform-digit/submission/friendsurance-friends-with-benefits [https://perma.cc/RDL8-CZJF].

[99] Danah Boyd & Kate Crawford, *Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon*, 15 INFO. COMM. & SOC'Y 662, 668 (2012) ("[T]hese errors and gaps [in big data] are magnified when multiple data sets are used together.").

[100] *See* Helfand, *supra* note 67, at 8 (stating that data "might be organized in a misleading or prejudicial way, it might be insufficient for the purposes to which it is put, or it might simply be incorrect . . . . Data also can be subject to influence or manipulation by third parties, especially when it relates to socially-constructed facts, such as what constitutes 'normal' or 'correct' behavior in a given situation.").

[101] *See* Gary Marcus & Ernest Davis, Opinion, *Eight (No, Nine!) Problems with Big Data*, N.Y. TIMES (Apr. 6, 2014), http://www.nyti.ms/1kgErs2 [https://perma.cc/AS42-LTWT]. We note there can also be algorithmic bias based on those coding the algorithms.

[102] Swedloff, *supra* note 11, at 356–57 (Big data can be "harvested without consent and often without the knowledge of the content generators").

guarantee that the personal identity is scrubbed from the data.[103] Data may be used to skirt anti-discrimination laws by directing online marketing to certain demographics of insureds, including race, gender, age, etc.[104] If insurers are prohibited from asking these types of information directly, they should not be allowed to collect or use them in risk classification, and efforts must be made to detect and prevent algorithmic discrimination.

Many concerns arise from the personalization aspect of underwriting. AI and big data increase the risk of unintentional but "rational" proxy discrimination.[105] While insurtech is dynamic and the correlations it discovers can be used to charge insurers accurate prices, some of these correlations are driven by factors that the consumer has little control over, leading to preferential treatment by the insurer.[106] That is, individuals with greater risk factors that usually would balance out as part of the risk pool might lose their subsidy and end up paying higher premiums. Premiums increase the more risk factors an individual has, and with the use of insurtech, underwriting is being done on the basis of smaller or more segmented categories of pools of risk.[107] Similarly, there are issues about who owns the data that the insured is producing for the insurer to use, particularly in situations where the insured is using wearable devices or telematic approaches.[108]

Hence, while not yet materialized, this personalization may ultimately leave some individuals without insurance if they cannot pay exorbitant prices, deeming them "un-insurables."[109] Federal and state regulators are attempting to assure

[103] *See id.* at 357 (stating "[w]hile the data is not necessarily used to identify specific individuals, personal identity is also not scrubbed from the data"); *see generally* Helveston, *supra* note 2, at 874 (stating digitally collected data could possibly not be permanently anonymized).

[104] Crawford & Schultz, *supra* note 8, at 99–100.

[105] Anya E.R. Prince & Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 IOWA L. REV. 1257 (2020) (arguing AI driven by big data are inherently structured to engage in proxy discrimination whenever they are deprived of information about membership in a legally suspect class whose predictive power cannot be measured more directly by non-suspect data available to the AI).

[106] *See* Max N. Helveston, *Reining in Commercial Exploitation of Consumer Data*, 123 PENN. ST. L. REV. 667, 681–82 (2019) [hereinafter Helveston, *Reining*] (noting the underwriting "can be driven by factors that the consumer had little to no control over").

[107] *Insurtech: Where Are We Now?*, *supra* note 93 (discussing the narrowing of the pool that insurtech allows for).

[108] With wearable devices or telematics in automobile insurance, the insured "is generating the data kept inside the device and policyholders might want some sort of control over what happens to that data." Swedloff, *supra* note 11, at 2063. Can the insured take this data to a new insurer or prevent the data from being shared with a new insurer? Further, "[i]f insurers own the data, it may make it more difficult to switch carriers, which raises additional concerns that insurers will charge their policyholders monopoly rates because the best insureds would have a hard time getting better rates without their data." *Id.* at 2064.

[109] Lewis, *supra* note 16, at 496; *Insurtech: Where Are We Now?*, *supra* note 93; *see generally* Ronen Avraham, Kyle D. Logue & Daniel Schwarcz, *Understanding Insurance*

prohibited factors are not being used by insurers when setting underwriting models and premium rates, especially when models are developed by data scientists as opposed to insurance actuaries.[110]

Further, insurtech may increase an insurer's control over an insured's behavior.[111] With the amount of data insurers can tap into, they may mobilize their enhanced knowledge over the insured and compel policyholders to engage in risk-reducing behaviors or face higher rates that inhibit the ability to maintain insurance.[112]

Many of the concerns raised in this section stem from not being able to see how AI and predictive models actually work, which creates a huge "black box" for policymakers, consumer advocates, and interested parties. Not having a transparent process for understanding how technology and big data operate leads to concerns that these technologies and models are having a disparate impact on protected

Anti-Discrimination Laws, 87 S. CAL. L. REV. 195, 217 (2014) (arguing that using suspect classifications "reinforces or perpetuates broader social inequalities or . . . causes some sort of expressive harm by acknowledging and legitimating that prior unfair treatment").

[110] For example, in 2019, the New York Department of Financial Services released a letter that states,

> [A]n insurer should not use an external data source, algorithm, or predictive model for underwriting or rating purposes unless the insurer can establish that the data source does not use and is not based in any way on race, color, creed, national origin, status as a victim of domestic violence, past lawful travel, or sexual orientation in any manner, or any other protected class . . . . An insurer may not simply rely on a vendor's claim of non-discrimination or the proprietary nature of a third-party process as a justification for a failure to independently determine compliance with anti-discrimination laws. The burden remains with the insurer at all times.

Susanne Sclafane, *Analyst Warns Regulatory Battle Over AI Bias to Grow; Lemonade Argues It's Fair*, INS. J. (Feb. 14, 2020), https://www.insurancejournal.com/news/national/2020/02/14/558440.htm?utm_content=technology-and-risk-management&utm_campaign=insuring-cannabis&utm_source=insurancejournal&utm_medium=newsletter [https://perma.cc/7YHX-2KM5] (quoting *Insurance Circular Letter No. 1 (2019)*, N.Y. STATE DEP'T OF FIN. SERVICES (Jan. 18, 2019), https://www.dfs.ny.gov/industryguidance/circularletters/cl20191). The letter also requires that insurers using these models explain why some insureds received higher prices than others, meaning there must be a causal story to explain why one insured is paying more for the same coverage than another.

[111] Helveston, *Reining*, *supra* note 106, at 675.

[112] For example, if high medical malpractice insurance premiums drive obstetricians out of the market, risk classification may be inefficient. Or people may choose not to get genetic testing even if there is a possibility that the information gained could help minimize the risk of future harm. *See* Alexander Tabarrok, *Genetic Testing: An Economic and Contractarian Analysis*, 13 J. HEALTH ECON. 75, 80 (1994).

classes.[113] To help inform the debate over the pros and cons of insurtech, we conducted the empirical research that follows in Parts III-V.

F. Fragmented Legal Regulations of Insurtech

Legal regulation of big data and AI use in the insurance industry are fragmented, weak, and limited at best. Federal law reserves to the states the authority to regulate the business of insurance.[114] In general, insurance state regulation focuses on establishing requirements for insurer advertising, licensing, solvency, residual pooling requirements, rate, and market conduct standards.[115] Companies and individuals involved in the insurance industry must obtain licenses for each state that they conduct business.

Many states are proactively fostering ways to help insurtech expand. Others are partnering with non-admitted insurers.[116] Connecticut, Kentucky, and Wisconsin

[113] If we cannot see what happens inside the "black box," then we "scrutinize what comes out of it. If the rates and underwriting criteria that predictive models produce are shown to have a disparate impact on protected classes, it's a safe bet such practices would be presumed 'unfairly discriminatory,' and it would be on the industry to show why they aren't." Ray Lehman, *Why 'Big Data' Will Force Insurance Companies to Think Hard About Race*, INS. J. (Mar. 27, 2018), https://www.insurancejournal.com/blogs/right-street/2018/03/27/484530.htm [https://perma.cc/LZM5-69SQ].

[114] 15 U.S.C. § 1012(a). The primary federal laws that directly govern insurance are found in the context of health and homeowners insurance through the Affordable Care Act, which limits what features an insurer can use in setting health insurance rates and explicitly precludes the use of other features such as gender, preexisting conditions, and genetic predisposition, and the U.S. Department of Housing and Urban Development's Fair Housing Act, which prohibits a facially neutral practice that may have a discriminatory effect in the housing market, including in insurance. Swedloff, *supra* note 11, at 2044–45.

[115] For a thorough background on the scope of insurance regulation, see Baird Webel & Carolyn Cobb, Cong. Rsch. Serv., RL31982, Insurance Regulation: History, Background, and Recent Congressional Oversight (Feb. 11, 2005).

[116] For an explanation of how insurtech companies take advantage of the non-admitted insurer market, see Zoe Sagalow, *Regulation Differs for Some 'Insurtech' Companies, GAO Says*, CQ ROLL CALL (June 11, 2019). Non-admitted insurers have not been approved by the state's insurance department and thus are subject to less regulation. Many states allow non-admitted insurers to conduct business only if they fill a need that admitted insurers are not equipped to handle, and any businesses or brokers that contract with non-admitted insurers must disclose to insureds that because these insurers do not contribute funds to the state guaranty fund, the insureds are not protected from the potential bankruptcy or insolvency of an insurance carrier. Hence, costs associated with this workaround include (1) in cases of insolvency, there are no guarantees that claims will be paid, even if a policy is active at the time of a transaction failure; and (2) if an insured believes his or her case was mishandled, there is no recourse available involving escalation to the state insurance department. *See id.* (identifying some of the regulatory issues insurtech companies encounter); *see generally* Andrew Bloomenthal, *Admitted Insurance Defined*, INVESTOPEDIA, https://www.investopedia.com/terms/a/admitted-insurance.asp [https://perma.cc/RG95-HFVP] (last updated Jan. 4, 2021) (comparing admitted and non-admitted insurance).

created "innovation offices" to respond to the growing demand for a fast track to develop, test, and get products to market.[117] Michigan even started a dedicated "hotline" to encourage insurers to work with regulators when developing new insurance products.[118] Despite these attempts to foster insurtech innovation and expansion, there is no unanimous approval concerning the role insurance regulation should play in this context.[119] To avoid the licensing requirements, many insurtech start-up companies are partnering with existing insurers and operating as a subunit within the larger, licensed insurer.[120] Critics express concern that insurance regulators are prioritizing insurtech expansion and are allowing insurtech companies to cut corners that traditional insurers cannot, thereby ignoring their primary duty of safeguarding the insurance marketplace.[121]

Recognizing the gap in oversight and regulation in the insurtech space, the National Association of Insurance Commissioners (NAIC) formed a series of task forces in the past four years to develop guidance on how the insurance field can deal with the rising interaction between insurance and technology.[122] It remains to be

[117] Chrys D. Lemon, Arshawn Teymoorian & Jeffrey M. Klein, *Two Industries Play in the Sand: Recent FinTech and InsurTech Developments*, 22(5) FINTECH L. REP. 1, 2 (2019) (highlighting expansive state approaches toward insurtech); Zoe Sagalow, *Connecticut Insurance Commissioner Launches Technology Advisory Council*, CQ ROLL CALL (Dec. 10, 2019).

[118] Andrea Miller, *Michigan Department of Insurance and Financial Services Encourages Insurance Innovation* (Aug. 9, 2018), https://www.michigan.gov/som/0,4669,7-192-26847-474834--,00.html [https://perma.cc/W95Y-WQDP].

[119] Lemon et al., *supra* note 117 ("[T]here is a sharp public policy divide developing between fostering innovation and protecting consumers.").

[120] Carlton Fields, *When Innovation Meets Regulation: InsurTech and State Licensing Laws*, JD SUPRA (Apr. 12, 2018), https://www.jdsupra.com/legalnews/when-innovation-meets-regulation-17232/ [https://perma.cc/6NXN-5FWC].

[121] Jason Hsieh, *INTERVIEW: How Insurance Tech Challenges Regulation to Keep Pace in U.S.*, THOMAS REUTERS (Aug. 28, 2019; 10:30 AM), https://www.reuters.com/article/bc-finreg-insurance-tech/interview-how-insurance-tech-challenges-regulation-to-keep-pace-in-u-s-idUSKCN1VH24N [https://perma.cc/R67K-38LZ] ("Some in the industry are questioning whether the concept of a regulatory sandbox for insurtech is even appropriate, arguing that allowing a technology company, but likely not a traditional carrier, to avoid certain insurance regulations, many of which are designed to protect the insurance-buying public, is antithetical to a regulator's primary duty to safeguard the insurance marketplace.").

[122] For example, the NAIC is the United States' standard-setting and regulatory support organization created and governed by the chief insurance regulators from all fifty states. It coordinates the regulation of insurers and develops national financial reporting, solvency, licensing, and market conduct standards. In 2017, the NAIC established the State Ahead strategic plan to provide services and resources to state regulators and created the Innovation and Technology (EX) Task Force to help regulators to stay informed and to "recognize the critical role they play in supporting innovation." GARY M. COHEN, 2 NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION § 8.10 (2020). The Task Force also sponsors Insurtech Summits and the annual Insurtech Connect Conference to provide a forum for insurtech startups to meet with regulators, showcase their products, and request various regulatory

seen what these task forces will recommend, but it appears they are focused on expanding insurtech in ways that do not compromise insurance regulatory goals.[123]

Thus, for the most part, state insurance laws were not created to address problems that result from technological advances from insurers' use of big data and technology. Very few laws and regulations directly address the role of big data and technology and meaningfully regulate insurers' use of big data and insurtech. Although there are some legal restrictions around privacy that insurers must comply with,[124] state insurers and the NAIC largely focus on ways to expand the insurtech market without compromising actuarial fairness. Because most of these regulatory initiatives are under- or newly developed, the impact on innovation and consumer protection is unknown.

Ironically, while normative debates over the role of these technologies rage, these debates are based largely on assumptions about what we *think* is happening. To date, we have little actual data on how big data, predictive analytics, and technology influence a particular industry, such as cyber insurance.[125] Using a

shortcuts so they can market and test their products. Mark Hollmer, *Big InsurTech Connect Conference Moves from Vegas to Virtual*, INS. J. (July 17, 2020), https://www.insurancejournal.com/news/national/2020/07/17/576000.htm?ref=insurancedailynews [https://perma.cc/S54C-Y77D]. Because the insurance industry is using big data, the Task Force oversees the Big Data (EX) Working Group, which gathers information to help regulators obtain a clear understanding of what data are collected, how they are collected, and how they are used by insurers and third parties in the context of marketing, rating, underwriting, and claims. The Big Data (EX) Working Group also explores opportunities for regulatory use of data to improve the efficiency and effectiveness of insurance regulation.

[123] To combat the issue of potential discrimination from the use of insurtech, the NAIC plans to form a Predictive Analytics Team (PAT) to both review complex pricing models and investigate "whether any variables in a rating plan are correlated with rating characteristics that are prohibited under state law." Helfand, *supra* note 67, at 17–18.

[124] For example, California in 2020 implemented the California Consumer Privacy Act of 2018 (CCPA), which protects consumers' privacy rights by (1) granting consumers the right to know what personal information is being collected about them and the right to know whether their personal information is sold or disclosed and to whom; (2) requiring companies to allow consumers access to personal information about them that businesses possess; (3) empowering consumers to prevent companies from selling their personal information; and (4) guaranteeing that those who exercise their privacy rights will be given equal services and prices as those who do not. Assemb. B. 375, 2017-2018 Leg., Reg. Sess. § 2(i) (Cal. 2017). It also puts data providers and insurers that do business in California on notice that they will have to manage their data in appropriate ways to not compromise consumers' privacy. *Id.*

[125] We note there has been some economic analysis of big data providers in the cyber insurance context, focusing largely on incidents, premium setting, and losses. *See generally* Sasha Romanosky, *Examining the Costs and Causes of Cyber Incidents,* 2 J. CYBERSECURITY 121 (2016) (examining the types of data these databases include, the costs of cyber incidents on companies that experienced them, and the causes of cyber breaches); Iñaki Aldasoro, Leonardo Gambacorta, Paolo Giudici & Thomas Leach, *The Drivers of Cyber Risk*, (BANK FOR INT'L SETTLEMENTS WORKING PAPER, No. 865, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3613173 [https://perma.cc/N3NQ-

mixed-method empirical design, the empirical study described below explores how cyber insurers manage uncertainty related to cybersecurity breaches and regulate the behavior of businesses concerning cyber risks using technology and big data.

II. METHODOLOGY

To maximize the internal and external validity of our research, we used several methods to explore the intersection of technology and cyber insurance. We outline our methods below.

A. Semi-Structured Interviews, Observations at Conferences, and Content Analysis of Insurance Applications

We conducted sixty in-depth, semi-structured interviews with members of the insurance field, including insurance underwriters, brokers, risk managers, actuaries, forensics experts, lawyers, data brokers, information security providers who actively partner with insurers, data scientists, and engineers who develop big data databases. We asked all interviewees about the role predictive analytics, big data, and emerging technologies play in the underwriting, pricing, and purchasing of cyber insurance, whether and how cyber insurer risk management services influence insureds' cybersecurity, and about best practices intended to improve cyber insurance and cybersecurity in society. Having conducted multiple interviews in virtually every category that makes up the insurance field, we feel confident that we captured the interplay between the insurance industry and technology and security. All in-depth interviews were confidential, lasted sixty to ninety minutes, and were digitally recorded and transcribed with the consent of the interviewees. To encourage candor, we agreed to not identify any interviewee. We used qualitative coding software,

TMRZ] (documenting the characteristics of cyber incidents based on an analysis of over 100,000 cyber events across sectors provided by a big data provider); Kjartan Palsson, Steinn Gudmundsson & Sachin Shetty, *Analysis of the Impact of Cyber Events for Cyber Insurance*, 45 GENEVA PAPERS ON RISK AND INS. 564, 564–79 (2020) (analyzing cyber incidents reported by one big data provider's cyber loss data feed and showing how type of incident relates to the eventual financial cost); COSTIS TOREGAS & NICOLAS ZAHN, GEORGE WASH. UNIV. CYBER SEC. POLICY & RSCH. INST. REP., INS. FOR CYBER ATTACKS: THE ISSUE OF SETTING PREMIUMS IN CONTEXT, REPORT-GW-CSPRI-2014-1 (2014) (discussing the challenge of premium setting with the insurance field and setting forth a research agenda for improving the cyber insurance policy premium setting process); Frank Innerhofer-Oberperfler & Ruth Breu, *Potential Rating Indicators for Cyberinsurance: An Exploratory Qualitative Study*, *in* ECON. OF INFO. SEC. AND PRIV. 249–78 (Tyler Moore, David J. Pym & Christos Ioannidis eds., 2010) (using qualitative interviews to identify a series of potential rating variables that could be used to calculate a premium for cyber insurance coverages); Antoine Bouveret, *Estimation of Losses Due to Cyber Risk for Financial Institution*s, 14 J. OPERATIONAL RISK (2019) (analyzing the main characteristics of cyberattacks and identifying patterns using correspondence analysis). Although these studies are helpful, there has been little interrogation of how these data are used by insurance brokers, carriers, and underwriters in making underwriting decisions and policy recommendations.

ATLAS.ti, to code the interview data. This allowed an additional layer of transparency, systematization, and formality to our coding process.

Over a period of four years, we also attended eight national conferences where the entire cyber insurance field comes together to discuss all aspects related to cyber insurance. Cyber insurance conferences are where the majority of actors involved in the drafting, marketing, buying, and selling of cyber insurance engage one another. These conferences allowed us to explore how the insurance industry thinks about data breaches and privacy laws, discuss the most important issues, and advise each other on best practices.

We also obtained and analyzed thirty cyber insurance applications from insurance companies that prospective insureds are asked to fill out. These documents allowed us to explore how insurers evaluate and account for a prospective insured's security measures in the underwriting process.

B. Analysis of Big Data Cyber Insurance Database

The biggest obstacle to conducting empirical research about big data and insurance is that information is difficult to obtain. Because cyber insurance is an emerging field, most brokers lack historical and actuarial data to assess cyber risk and price insurance. Insurance underwriters and brokers, therefore, rely on expensive, commercial, third-party databases developed by data providers that compile information on cyber incidents and losses. Today, cyber insurers rely on three to four major big data providers.

Despite the difficulty of accessing big data sources, we purchased access to one of the major databases that insurance companies and brokers use. The database contains more than 90,000 records from publicly available sources about cyber events and presents information about different types of cyber risks.[126] The data are organized into peer groups by company, industry type, and revenue amount. In addition to recording the parent company, company size, company type, and industry of each cyber event, the database also includes information about the number of records affected, the type of losses suffered, how the breach occurred, and the type of cyber risk posed.

Users seeking to sell or buy insurance may run simulations to understand the estimated impact a cyber breach may have on a company of a particular industry, size, and possession of a certain number of records. Brokers use such data to recommend policy limits for prospective buyers of insurance by running simulations on similarly situated buyers.

In order to understand how underwriters, brokers, and buyers rely upon the information presented in the database, we ran 300 simulations across various industry sectors, including agriculture, forestry, manufacturing, finance, insurance,

[126] Given the competitive market surrounding big data providers and the importance of anonymity, we agreed to not disclose the name of the database that we accessed. To assure anonymity, we inserted ["a data provider"] instead of the actual company name where interviewees reference any data provider.

and health care.[127] We focused on observing patterns and inconsistencies in visual information presented in the database and assessing the utility of the database for buyers of insurance in determining whether and how much coverage is appropriate, with a recognition of how such information is presented in the database.

Most important, we attempted to identify whether the database is used as a tool to encourage buyers to purchase higher limits of coverage (and, therefore, pay more premiums). In sum, we believe our mixed-method approach allows us to explore the processes through which predictive analytics, big data, and emerging technologies transform the delivery of insurance as well as the implications and effects of such practices for broader topics such as consumer privacy and algorithmic justice in society.

III. THE TECHNOLOGIZATION OF INSURANCE

The following highlights the technologization of insurance and the process whereby the practice and delivery of insurance (underwriting and risk and claims management) is influenced and shaped by technology. Insurance companies and brokers, the two key actors in delivering cyber insurance, are managing the uncertainty of evaluating cyber risk by using big data, AI, and other technologies. Insurance brokers play an important intermediary role. In particular, brokers represent interested buyers of insurance and generate business by connecting their clients with insurance companies offering coverage.[128] Insurers also use technology to regulate the behavior of their insureds, attempting to nudge them toward greater risk management and prevention through risk and insurance. Or, at least, that is one of their goals.

A. Managing Uncertainty with Technology in the Insurance Field

Cyber insurers and brokers face the especially difficult task of assessing risk with a lack of reliable actuarial data that has developed for other lines of insurance. Whereas automobile, property, and commercial general liability insurance can rely on decades of predictive data to assess and evaluate risk, the relative lack of information makes cyber insurance risk evaluation far less certain. In addition to the

[127] These industries reflect a broad cross-section of companies that frequently experience cybersecurity breaches.

[128] Insurance brokers do not work for insurance companies and cannot bind businesses, i.e., by entering into an insurance contract on behalf of the insurance company. Rather, brokers direct clients to insurance agents or directly to insurance companies, with whom the clients can enter into insurance contracts. Brokers do have a financial stake in the transaction, in the form of commissions earned on policies that they bind or place. For background on the role of insurance brokers, see generally *Insurance Agents and Brokers*, INSUREON, https://www.insureon.com/insurance-glossary/insurance-agent-broker [https://perma.cc/R5KZ-F78J] (last visited Jan. 25, 2020); Marianne Bonner, *How Insurance Agents Make Money*, THE BALANCE SMALL BUS. (Sept. 9, 2019), https://www.thebalancesmb.com/agents-versus-brokers-and-how-they-make-money-462383 [https://perma.cc/FHJ9-FM9J].

lack of data, cyber attackers constantly modify their tactics as adaptive adversaries. Data breach, phishing, malware, and social engineering are just a few of the ways cybercriminals attack consumers. Virtually every industry has fallen victim to cybersecurity incidents. Businesses, governments, and ultimately insurers are having trouble keeping pace.

One key problem with cyber insurance underwriting is the relative lack of expertise of those filling out applications on behalf of potential insureds. As a result, many of those in our study believe applications alone to be an incomplete and unreliable tool for evaluating the risk profile of a prospective policyholder.[129] Because insurers face significant uncertainty concerning how to price cyber risk, they are turning to technology:

> I've been surprised at the level of sort of big data and predictive analytics that it seems like insurers are using, brokers are using. There are third-party companies [that are data providers] that market this information. And that seems like it's playing a big role and an increasing role in part because there's not a lot of good data on cyber.[130]

Insurance brokers themselves are desperate for reliable data: "I think . . . cyber brokers and agents will take anything that they can get because, for a long time, we haven't had very much."[131]

Our interviews reveal that today, many insurers' decisions on whether to issue a policy to a particular insured, and whether and how to underwrite the risk, largely hinges on the use of big data, technology, and AI. Information security and forensic companies and big data providers have penetrated the cyber market using technology tools. Although there are a handful of big data providers harnessing loss data and aggregating such data, the insurance field is flooded with information security and cyber forensics companies to assist insurers with underwriting and risk and claims management. Some large insurance companies rely on their own big data

[129] *See* Interview 27, Insurance Coverage Lawyer (on file with author) ("In my view, it's that insurers are still trying to figure out how to evaluate the risk. They're not quite sure how to really monetize what the granting of any particular coverage is."). In addition to uncertainty due to lack of claims history, insurers rely on technology because:

> the applications aren't necessarily getting the entire job done. And there's a few different issues there. One is you're not necessarily going to get a fully filled out application . . . . [Also] [w]ho's filling out this application? So, if someone from cybersecurity within a company is filling it out, you're going to get very different answers than if the CFO's filling it out. . . . And so the quality of the data that you're capturing is still pretty uncertain. [Y]ou don't necessarily get an opportunity to ask those follow-up questions for various reasons.

Interview 36, Information Security Provider (on file with author).

[130] Interview 15, Cyber Insurance Attorney (on file with author).

[131] Interview 22, Wholesale Broker (on file with author).

and have hired security and forensics engineers to develop their own information security tools. However, our interviews reveal that the majority of insurers are contracting with a variety of information security providers and big data providers rather than hiring these skills in-house. Facing similar challenges, insurance brokers have resorted to a variety of big data, predictive analytics, and security tools to help assist clients seeking cyber insurance.

Many insurance brokers and risk managers (who buy insurance for their clients) indicated to us that they find the insurance application's rigid, mechanical, check-the-box format inadequate for the prospective insurance buyer to accurately communicate the company's cybersecurity posture. Particularly for small and middle-market companies (SMEs) (with revenue of less than $250 million), security scans conducted by insurance companies or, more often, third-party information security companies that contract with insurance companies, are displacing the "old" methodology of evaluating and verifying insurance applications and follow-up meetings between the insurer and the potential insured. Perhaps unsurprisingly, large, wealthy organizations continue to have the luxury of a much more "high-touch" approach that often includes scanning and evaluating the potential insured's visible cyber risk but is supplemented by a closer evaluation of the insurance application and follow-up meetings to discuss in detail the customer's cyber risk profile and mitigation efforts. These follow-up meetings offer the opportunity for a meaningful discussion to occur regarding the cyber hygiene of the organization, as well as the opportunity to conduct real bargaining over the terms of the insurance.

Indeed, our interviews suggest that numerous well-heeled and sophisticated companies even hold their own competitions among potential insurers when deciding to purchase cyber insurance. After demonstrating to multiple potential insurers their company's cybersecurity posture, large corporations choose among bids from multiple cyber insurers pitching their services. As such, a number of insurers we interviewed noted that risk managers and other buyers of insurance, particularly at large companies with revenue above $250 million, expect the insurer to understand technology in order to fully understand how to evaluate the risk of the buyer and how to price the risk.[132]

We now explore more precisely how big data, AI, and emerging technologies are changing the business of cyber insurance.

B. Data Brokers Aggregate Data on Claims and Events that Have Already Occurred

Data brokers collect information on thousands of claims and losses from public records and nonpublic information from brokers and insurers and then sell the

[132] Sophisticated buyers of insurance, according to many cyber insurers, understand technology: "Th[e] conversation's gotten to a point where [if] you're way out of your depth, you can't come in here and sell me an insurance policy if you don't understand what I'm telling you about my technology infrastructure. So that's sort of changing a bit." *See* Interview A10, Insurer (on file with author).

aggregated information back to insurers and brokers attempting to understand the extent of the cyber insurance market and types of breaches that may be reasonably expected.[133] Insurance brokers and companies also buy big data from data brokers in order to develop pricing and underwriting models.[134]

Through collecting and analyzing information on cyber breaches, including loss amounts and type of information lost, big data allow insurers to explore the scope of cyber events in a way not previously possible. For example, for specific peer groups selected, the database we analyzed provides details about prior cyber events experienced by similar companies, including the dates of prior breaches, amount of records lost, type of breach, and actual or estimated cost of the breach to the victim companies. This allows insurance underwriters and brokers to understand the frequency of breaches in that peer group, and what type of data have historically been affected—and through what type of breach. They can then compare that with information about the company seeking insurance.

While not necessarily predictive of risk, such historical information can lend reliability to decisions to insure and to the price points for various cyber insurance options. One executive of a large insurer noted that most large insurers purchase big data but rely primarily on data acquired about their own insureds, whereas smaller insurers often rely heavily on purchased big data to enhance their models: "[It's] more helpful for companies that don't have as substantial a book of business, if I'm being honest."[135]

Insurance brokers that we interviewed routinely noted that these aggregated databases allow brokers to provide to their customer companies "detailed analysis of where some of their peers may be purchasing, what type of limits are being put up and then how much [is reasonable to pay] based on client claims data from our carriers."[136] These data also have the potential to influence a prospective buyer of insurance to purchase specific amounts of coverage and limits based on what similarly-sized organizations in the same industry have bought.

Brokers routinely present findings from big data analytics directly to clients to help prospective buyers understand why a broker is recommending coverage at particular parameters: "When we are pitching a client, we can say, 'We have thirty-five or forty other retail or health care organization clients that we work with that kind of have a similar profile from a revenue standpoint, record standpoint, control

[133] Interview 35, Underwriter (on file with author) ("[Big data providers] are kind of aggregating claims data and then, you know, providing trends of you know, like law firms are more likely to get hit than manufacturing firms by a cyberattack. And when they do [get breached], the average cost of a claim is X . . . . [They are] aggregating stuff that has already happened.").

[134] *See* Interview 33 Part 1, Data Aggregator & Big Data Provider (on file with author) ("[T]he data is being used to create pricing models . . . . It is also being used to create more granular pricing underwriting models as well.").

[135] Interview 35, *supra* note 133; *see also* Interview 4, Underwriter (on file with author) ("Currently, right now to price the risk you're definitely using outside data along with your own, and you provide [the insurance] on a non-admitted policy form.").

[136] Interview 23, Wholesale Broker & Underwriter (on file with author).

standpoint.'"[137] Big data providers are providing insurers and insurance brokers with aggregate data about breaches that have already happened to similarly situated organizations. Thus, big data from these entities fuel the expansive use of technology, analytics, and AI in the cyber insurance field.[138]

C. Information Security Companies Drive Sales with Aggregate Risk Analysis

Relying partially on big data, a growing number of information security companies[139] are focused on modeling aggregate or systemic risk to an insurer's portfolio:

> [It] is more geared to aggregation, and what they're doing and doing pretty well is to say, "Okay. If this kind of scenario happened, you might have a portfolio of 30,000 customers, and 5,000 of those 30,000 are all using the same cloud provider," and maybe we [the insurer] don't know that, but maybe [the information security company] can help us understand that.
>
> [T]hen we say, "Aha. Are we comfortable with that kind of potential aggregation?" Because if those 5,000 customers maybe don't each [have a data breach] event, but they're reliant on the same vendor and that vendor has an event that could cause a ripple effect on our [insurance] portfolio. So, they help model out both kinds of those scenarios and what that looks like across a portfolio of business.[140]

Information security companies evaluate the insurer's client population and then use analytics and modeling to evaluate aggregate risk. These security companies use technology, security, and insurance experts to understand aggregate risks:

[137] Interview 3, Broker (on file with author).

[138] Big data providers that we interviewed were not hesitant to recognize the importance of their data for the cyber insurance field:

> Interviewer: [I]s it fair to say [that providing the data], the underbelly of the insurance lifecycle here for cyber, is based in part on [the information that your company] has compiled?
> Data broker: Yes, I think that's fair to say.

Interview 33, Part 1, *supra* note 134. Moreover, AI and other emerging technologies rely on big data to generate outputs.

[139] Some of the major companies in this area include RSI, RSM, Cyber Cube, Insight Cyber Group, and Symantec. *See, e.g.*, Helen Yates, *Cyber Solutions 4.0: Modeling Systemic Risk*, EXPOSURE MAG. (May 5, 2020), https://www.rms.com/exposure/cyber-solutions-40-modeling-systemic-risk [https://perma.cc/876A-F8L8].

[140] Interview 35, *supra* note 133.

> [I]n-house we have people like me who are actuaries, underwriters, brokers. And then we have the . . . cybersecurity experts, intelligence experts, [and] economists. And so, we have all these professionals sitting under the same roof who have been trying to speak the same language and solve this problem together. We've got the experts there.[141]

To convince buyers to purchase insurance and avoid worst-case scenario exposures, insurers use these tools to translate data and analytics into risk avoidance and cost containment:

> I think that the common language is dollars and probabilities. And that's what the boardroom can respond to. If I'm the technical IT guy and I come to you and say we have two million botnets on our network and 500 high severity vulnerabilities, and you are a board member, you're going to look at me and say, "I have no clue what that means."
>
> But if you come to me and you say, "Sir, we believe that there's a 1 percent chance that we have any of these events occur in the next 12 months. And the worst-case scenario is a billion-dollar loss." That's a much different conversation. That's the way that you can corral resources and start to actually manage the risk and manage the exposure and not have kind of these blind-siding type events.[142]

Technology and big data tools, therefore, are driving the insurance sales process by translating aggregate risk into a language that buyers of insurance understand: potential profit and loss.

D. Information Security Companies Assist Insurers in Evaluating Risk of Prospective Insureds Through Cybersecurity Health Evaluations and Scans

Other information security providers are contracting with insurers to evaluate the cyber hygiene and vulnerability of prospective insureds.[143] These companies are less concerned about the aggregate, systemic risk to an insurer's large portfolio of clients. Instead, they focus on individual companies looking to buy insurance, giving each a score or rating that helps underwriters determine the risk level of a specific company and whether they want to issue insurance to that company:

[141] Interview 36, *supra* note 129.

[142] Interview 32, Insurer & Information Security Provider (on file with author).

[143] Cyber hygiene refers to the ways that individuals and organizations protect and maintain IT systems and devices and implement cybersecurity best practices. For example, an organization using the best cybersecurity practices has a strong or healthy cyber hygiene profile. For more background on cyber hygiene, see Tony Sager, *Cleaning Up a Definition of Basic Cyber Hygiene*, CTR. FOR INTERNET SEC., http://cissecurity.org/blog/cleaning-up-a-definition-of-basic-cyber-hygine [https://perma.cc/5L2Q-FG24] (last visited Feb. 1, 2020).

> [Cyence, BitSight, and Security Scorecard are] more looking specifically [whether] this particular company, ABC Inc., has a vulnerability because they have a poor patching cadence. And we know they have poor patching cadence because they're still running software that's facing the internet that hasn't been patched. So, they're telling you more specifically about an individual account . . . .[144]

Using security and technology tools, these companies conduct endpoint vulnerability assessments and provide a rating or score based on information gathered from a company's IP address, domain name, and other publicly accessible information, as well as on information about the company posted on the dark web.[145] One information security provider referred to these companies as an "intelligence service for the underwriters . . . . A lot of times the clients have no idea."[146] A big data provider we interviewed noted their data are often used to validate information produced from the security provider's scoring systems: "Companies that do scoring based on various attributes of a company's cybersecurity profile—they use our data to demonstrate the veracity of their scoring systems."[147] One information security provider has the ability to go "inside" the company's firewall to evaluate the cybersecurity of the company.[148] This information security provider told us:

> [W]e have exclusive rights to [the data from] . . . one of the largest security companies in the world. We're the only ones that have it, and that's going to give us data that's from inside the firewall. So, we're not just doing network scans and looking from the outside in. We can also look from the inside out. Now, [the security provider we work with] has to anonymize and aggregate this, so we get it on what we call microsegment level. So,

[144] Interview 35, *supra* note 133.

[145] The dark web refers to encrypted online content that is not indexed by conventional search engines. Although the dark web assists people who want to maintain privacy and freely express their views, the dark web has also gained a reputation as a haven for illegal activities. For more background on the dark web, see Andrew Bloomenthal, *Dark Web*, INVESTOPEDIA (June 13, 2021), http://www.investopedia.com/terms/d/dark-web.asp [https://perma.cc/7E78-QZ65].

[146] Interview 16, Forensic Security Consultant (on file with author).

[147] Interview 33, Part I, *supra* note 134.

[148] Vulnerability scanning is a technique used to identify potential vulnerabilities in an organization's information system and hosted applications. Such scans attempt to identify vulnerabilities such as software flaws, lack of updated security patching, and improper firewall or other system configurations. *See, e.g.*, *NIST Special Publication 800-53 (Rev. 5.1)*, NAT'L INST. OF STANDARDS & TECH., (June 16, 2021) https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control?version=5.1&number=RA-5 [https://perma.cc/NBS5-UFPZ]. As the names imply, an *external* scan may be conducted from any location with an operable internet connection against the parts of an organization's IT infrastructure facing the internet, whereas an *internal* scan must be conducted from inside an organization's firewall. The vast majority of information security providers conduct external scans. *Id.*

> it's groups of companies that have the same kind of profile. [It] looks at region, revenue band, and industry.
>
> We still believe that's still very helpful. And the insurance industry is very comfortable looking at risks on a homogeneous risk basis . . . . We also work with . . . up to ten or twelve companies that we're contracted with to grab other data. And a lot of that is outside the firewall—so, network scanning of different kinds.[149]

In addition to assisting with pricing, insurers believe the scores increase their efficiency and accuracy in pricing and the specific terms they offer in cyber insurance policies, rendering the insurance application answers less important:

> [I]f somebody has a good cybersecurity hygiene, I can rely on third-party data to help me, which makes it more convenient for the customer because they don't have to fill out a lengthy application. I don't have to worry about does the person filling that application out even understand the question I asked them? Are they just checking "yes" because they feel like a "no" would result in a bad outcome? So, it's easier. It's more accurate. It's more granular, and I can then set my pricing more accurately to reflect that individual risk.[150]

Insurers engaging large organizations often use the security score to have a deeper conversation with their clients about cybersecurity.

Insurance brokers working with large organizations also contract with security organizations to scan networks of prospective insureds to evaluate their vulnerabilities. The security organization issues a score that can be used to help the insurance broker counsel the prospective insured on their cyber hygiene and the likelihood of coverage: "[W]e do partner with some firms from an outsider's perspective that . . . scan . . . their network from the perimeter to see where there may or may not be some vulnerabilities . . . . But the score is very helpful for just having a dialogue with the client."[151]

According to our interviewees, some insurance brokers graft the information security firms' risk ratings and factors onto their own model for marketing purposes: "If you look at insurance brokers . . ., for example, . . . [w]hat they do is they use our analytics, and then they take their expertise, provide consulting services and really use it as a tool in theirs."[152] Virtually all insurance industry actors we interviewed indicate insurance companies need big data, AI, and other technologies that the information security companies provide in order to stay viable: "[U]nderwriters are

[149] Interview 36, *supra* note 129.

[150] Interview 35, *supra* note 133.

[151] Interview 10, Broker (on file with author).

[152] Interview 32, *supra* note 142.

now recognizing [that they] . . . need to have one or more of those tools in the shops to be able to continue to be competitive in the marketplace."[153]

E. Artificial Intelligence as a Tool for Increased Insurance Company Efficiency

The technologization of insurance involves not just big data, predictive analytics, and advanced security and forensic tools. Our interviews reveal that AI plays an increasing role as well. Information security providers use AI to assist insurers with building predictive models to enhance efficiency in the underwriting process. One of the leading information security providers highlights the connection between big data, AI, and the insurance underwriting process:

> And so, what we did is we started collecting all that data, as well as looking at things like dark web data, and building out machine-learning algorithms and natural language processing algorithms to actually sort through all this stuff at scale. And so now, instead of only having your population of companies that you've either underwritten and actually written the policy or have come and shopped with you, you can now compare people to the universe and use that to really try to fine-tune your strategy.
>
> So, underwriters can get company-specific information—sets of risk factors, technical things like vulnerabilities to behavioral things like employee sentiment, for example. And then we'll build out frequency and severity models and provide analytics on all this stuff so that underwriters could understand if I write a particular layer of coverage, based on [these] models, what are the dollars and probabilities associated to losses?[154]

This interview excerpt highlights the technologization of insurance. It reveals the interconnection between big data, AI, and the predictive analytics that mobilize such data and, most importantly, the manner in which insurers *operationalize* such data in the delivery of insurance. Insurance companies are short-circuiting the traditional underwriting process and are able to "plug in" information from a prospective buyer of insurance and receive a report geared toward assisting the insurer with pricing the risk: "[O]ther people that are taking those risk assessments that we do on an individual company basis and using them kind of more loosely in their guidelines, using it to dictate [underwriting] authority . . . . There's people that are working it into their underwriting guidelines."[155]

[153] Interview 33, Part I, *supra* note 134.

[154] Interview 32, *supra* note 142. Other insurance officials suggest insurers and information security providers engage in more machine learning and natural language processing than predictive analytics. *See* Interview 33, Part II, Data Aggregator (on file with author) (noting that insurers and information security providers are "using machine learning and, to a lesser degree, natural language processing to be able to rate, quote, and bind nearly instantaneously for small businesses").

[155] *Id.*

Thus, the traditional underwriting process for most non-cyber lines of insurance, anchored by the insurance application, client consultation, and loss actuarial history built over decades, is supplanted by relying largely on information security companies that are partnering with insurers and using big data, AI, and other predictive analytics. Brokers manage the uncertainty of cyber risk by also relying on these tools to evaluate the risk profile of the prospective buyer of insurance and to better gauge the level of insurance policy limits they recommend be purchased.[156]

F. Insurers Use Big Data, AI, and Other Technologies to Engage in Risk Management and Loss Prevention

Given that most organizations are under-compliant with privacy laws and underprepared for cybersecurity breaches,[157] cyber insurers engage in risk and loss prevention on behalf of the organizations that purchase their insurance. By attempting to prevent, detect, and respond to cybersecurity breaches, insurers play a *de facto* regulator role. Insurers offer a series of pre- and post-breach services to purchasers of cyber insurance. Cybersecurity conferences heavily promote cyber insurance by focusing on the availability of what they refer to as "value-added" pre- and post-breach services.[158]

Pre-breach services focus on preventing and detecting risks to the organization. Insurers offer new policyholders access to a series of risk-prevention tools they claim will reduce their company's likelihood of falling victim to a cyberattack.[159] Once an insured purchases a policy, they gain access to a portal of tools, ranging from training, written materials, incident response plans, software, free virus-scanning capability, password management, and most important, consultation with forensic and information security companies that insurers contract with: "Our real focus has been partnering with all the major insurance companies that offer cyber

[156] High-touch brokers use technology to supplement the evaluative process, whereas some low-touch brokers rely on data and security scans as a substitute to the traditional broker-buyer relationship.

[157] Talesh, *Compliance Managers*, *supra* note 18, at 419, 428–33.

[158] *See id.* at 428–29.

[159] The following highlights one example of the bundle of pre-breach services that insurers make available to insureds:

> We help customers build breach response plans that . . . they can access . . . from their iPhone at a moment's notice and connect in with a breach coach lawyer and their forensics expert and all that. The assessment side is consulting, it's pre-breach . . . . There's also a lot of proactive stuff inside that portal like calculators that show them what a future data breach is going to cost them, online security training for their staff, things like that.

Interview 16, *supra* note 146.

risk insurance coverage of some flavor . . . . We are essentially their loss control partner, helping to assess the risks of their customers, their cyber and privacy risks."[160]

Insurers alert new insureds that these services are available should they choose to use them. However, insureds are not required to use these services. There are dozens of information security providers fighting for market share in this area, each offering products they believe help insureds reduce the chance of a data breach event occurring.[161] In theory, these risk prevention tools and security ratings encourage better cyber hygiene and resiliency by insureds.

Insurers also provide access to post-breach services "aimed at responding to, investigating, defending, and mitigating against the consequences surrounding a data breach event or privacy law violation."[162] Insurers contract with third-party vendors that the insured can use, or they have in-house units to provide such services. In many cases, cyber insurers are providing risk response well beyond the scope of what insurers in other lines typically handle and are becoming, in effect, compliance managers for their insureds.[163] Post-breach services offer insureds the services of law firms, forensic analysts, crisis management businesses, and credit monitoring companies approved by the insurer.[164]

In sum, this Part reveals how pervasive the technologization of insurance has become in the cyber context. Insurance companies and brokers have embedded big data, AI, and other technology tools in the delivery of insurance. Part IV explores the implications of this technologization.

[160] *Id.*

[161] Interview 33, Part II, *supra* note 154. ("They are either companies with products specifically targeting the cyber insurance marketplace or . . . information security providers of various sources who have products they believe would be useful in the cyber insurance space.").

[162] Talesh, *Compliance Managers*, *supra* note 18, at 432. For a deeper exploration of cyber insurer post-breach services, see *id.* at 432–35.

[163] *See id.*

[164] Our interviews explored the post-breach services offered, and we briefly highlight them here. Insurers provide organizations access to a suite of post-breach services, often at a discount or premium reduction, including designated panels of lawyers to assist in managing legal issues that arise when a data breach occurs. In addition to legal advice and guiding the organization on how to deal with the cybersecurity incident, they advise organizations on how to mitigate regulatory fines and liability for data breaches. In this respect, insurers are shaping the way organizations comply with privacy and cybersecurity legal challenges on the ground either directly or through third-party vendors, access to—and coverage for—forensic and other cybersecurity experts. These experts help organizations identify the sources and causes of a data breach, contain the breach, and ultimately restore the network processes that may have been damaged as a result of the breach, as well as help mitigate the risk of additional attacks. Insurers also provide access to pre-approved public relations and crisis management firms. These firms provide notification, advertising, and related communications assistance to help protect and restore the insured's reputation following a breach event. For a deeper exploration of cyber insurer post-breach services, see *id.* at 432–35.

IV. WORTHY GOAL—LACKLUSTER RESULTS: BIG DATA, AI, AND EMERGING TECHNOLOGIES HAVE YET TO IMPROVE OVERALL CYBERSECURITY

Our research suggests, somewhat surprisingly, that insurtech interventions and innovations, while they may have benefits for the efficiency of the cyber insurance industry, are largely ineffective at enhancing organizations' cybersecurity. To the extent insurers are attempting to fill a regulatory void, they do not appear to be doing so effectively.

A. Big Data in the Cyber Insurance Context Is an Unreliable Tool

Despite increasing the amount of information that buyers and sellers have access to in the cyber context, the big data database we accessed and examined reveals that the data are limited and not always accurate or reliable. To begin, the quality and sources from which information is compiled are limited and paint an incomplete picture of any particular peer group's cybersecurity posture and associated risk. This is largely because the database relies upon publicly available data to create sets of peer groups. Hence, there are events the database does not record. In other words, just because the database only includes a few cyber events in a specific peer group does not necessarily mean that peer group is less prone to cyber events. Rather, it could mean that cyber events experienced by companies in that peer group are not generally public or do not make their way into the public domain by way of reporting or lawsuits, or those compiling the database simply did not find some of the incidents.[165] Because cyber insurance lacks a mandated, standardized, and/or centralized line of reporting, no source of information is complete, and disparate sources contain different types and amounts of data.[166] Moreover, this information may be especially selective and unrepresentative because large insurance companies use their own data sets of cyber losses when pricing insurance, purposely excluding incidents of their insureds from public record databases.

The varied type and quality of the data used by insurance-related data providers is a major concern. Many insurers do not share their data with big data providers for fear of losing a competitive advantage in the market. The following describes the privacy concerns that insurers maintain:

> But [we're] not going to give [a data provider] our data. And a lot of insureds don't want this stuff to go public. They're not publicly traded, or they don't have to answer to a regulator, they're going to close it out. They'll do their notification and unless somebody happened to write a

[165] As one underwriter noted in an interview, "You don't really know what anything costs unless it was a publicly-traded company." Interview 12, Underwriter & Risk Manager (on file with author).

[166] Although most states require organizations to notify customers when a breach occurs, there is no law requiring insurance companies to share data on cyber attacks.

> newspaper article about it, your [big data provider] people aren't going to find it . . . . [They're] basically throwing darts . . . .
>
> Most of the stuff, most of the breach responses are done under privilege with counsel. They don't want to share with the FBI to track down the criminals, let alone share with some public actors putting together a database to talk about numbers. So, they're just trying to bring in data from any point they can get. But it's still so early in the ballgame that it's really hard to get there.[167]

Moreover, the database we examined is entirely backward-looking, i.e., trying to offer benchmark recommendations on policy limits based on events in the past that do not account for changing cyber threat patterns.[168] Many brokers and industry leaders we interviewed critiqued this benchmarking approach by big data providers because it is backward-looking and unreliable:

> And they always say [they'll] give me some benchmarking. Well, I mean, I get so angry whenever I hear that . . . . So, you've got this evolving threatscape in front of you, and you're going to drive the car by looking in the rearview mirror to see what the clowns behind you, who are just as blind as you, are doing? It's crazy. So, I would say no, benchmarking is useless, do a ground-up analysis.[169]

Another insurance industry expert noted: "[D]ata benchmarking to evaluate limits is not too reliable. [It's] [o]kay to use a little but don't rely on it exclusively."[170]

Limits and deficiencies in the data used by insurance-related data providers have several negative implications. Because these databases often rely on reported losses, there may be certain types of events affecting a company's cybersecurity posture, as well as risk unaccounted for in any policy for cyber insurance that used a database relying on an incomplete source of data. A forensic security expert also questioned the reliability of third-party databases like the one we evaluated for this study, indicating that such data did not align with "what we're seeing in the insurance world."[171] As one insurance industry expert stated: "For me, the big issue is the credibility and the source of the data."[172] Hence, although all agree that big data providers are fueling the rise in AI and predictive analytics usage in the cyber context, our analysis calls into question the robustness and completeness of the data and suggests that it is likely insufficiently reliable to form a rational basis for the

[167] Interview 31, Insurer & Big Data Provider (on filed with author).

[168] Benchmarking involves estimating what the potential loss could be if different scenarios happen to a prospective buyer of insurance.

[169] Interview 12, *supra* note 165.

[170] Interview 54, Broker (on file with author).

[171] Interview 16, *supra* note 146.

[172] Interview 37, Insurance Industry Expert (on file with author).

number and significance of cyber insurance decisions being made based on such data and analysis.

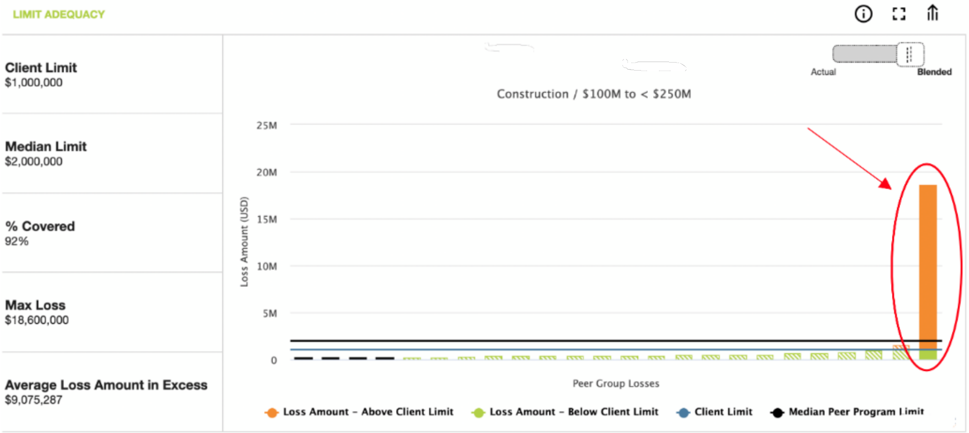
B. Data Broker Databases Are Being Used by Brokers and Underwriters to Nudge Clients Towards Purchasing More Insurance

One could argue that any large amount of data—even if admittedly incomplete and flawed—is better than nothing and that the incompleteness is not the fault of the data providers or the result of unsavory motivations on the part of any participants in the cyber insurance ecosystem. Our research, however, uncovered a more insidious problem with the use of big data in cyber insurance. Careful examination of the data broker's database reveals that they do not discount outliers of excessive loss amounts when presenting or calculating key statistics. Throughout our analysis of various peer groups, the database consistently included outlier loss amounts experienced by companies in a particular peer group in presentations of data through figures and in calculations of key summary statistics. In other words, the database inflates the potential cost of losses and nudges buyers of insurance to purchase more limits.

Figure 1 shows how not discounting outliers impacts insurance policy limit recommendations for prospective buyers of insurance. After users select the industry type, revenue range, premium, limits, and retention amounts, the database presents users with a chart. This chart reveals prior loss amounts experienced by, and median limits of, companies in the selected peer group (based on industry type and revenue range).

However, when plotting this information, the database does not discount either low or high outliers in the data of loss amounts. Especially when the data include a high outlier, a visual inspection of the plot suggests that a company may experience a much higher loss than average and thus would significantly raise the insurance coverage limits on the policy (and, in turn, require buyers to pay higher premiums). In Figure 1, there is one outlier, as evidenced by a bar circled on the right. Through a quick and cursory visual inspection, a user may be misled to believe that a high loss amount is more common than not or that the maximum loss amount is higher than it actually is.

Figure 1



LIMIT ADEQUACY

Client Limit
$1,000,000

Median Limit
$2,000,000

% Covered
92%

Max Loss
$18,600,000

Average Loss Amount in Excess
$9,075,287

Actual
Blended
Construction / $100M to < $250M
25M
20M
15M
10M
5M
0
Loss Amount (USD)
Peer Group Losses
Loss Amount – Above Client Limit
Loss Amount – Below Client Limit
Client Limit
Median Peer Program Limit

Figure 1. This figure presents the chart that insurance brokers present to prospective buyers after they select a particular peer group and choose a client limit. In this case, one outlier breach significantly raises the maximum loss estimate. On the right side of the chart, each bar represents a prior cyber event the database has recoded. The light blue horizontal line represents the client's chosen limit. The back horizontal line represents the median limit of policies obtained by companies in the selected peer group. The left panel presents a series of summary statistics that tell the user (1) the client's selected limit, (2) the median limit of policies held by companies in this peer group, (3) what percentage of the losses plotted would be covered under the client's selected limit, (4) what the maximum loss amount recorded is among companies in this peer group, and (5) the average loss amount that exceeds the client's chosen limit.

The database presents the "average loss amount in excess" and "max loss" in the pane on the left—accounting for the outlier. Under this format, the maximum loss estimate is $18,600,000, and the average loss amount in excess of the $1,000,000 proposed limit is $9,075,287. The average loss amount in excess is the difference between the limit chosen by the client in creating the simulation and the average of all losses recorded in the database that are greater than that limit. Even though there are only two losses greater than the client's selected limit of $1,000,000 in Figure 1: With a loss event estimated to be $1,550,574 and the outlier event of $18,600,000, the "average loss amount in excess," (the difference between of these two numbers—$10,075,287—and the client's chosen limit of $1,000,000) is $9,075,287 (see left panel of Figure 1). In other words, this figure suggests the average loss amount in excess of an insurance policy limit of $1,000,000 for a particular buyer will be over $9,000,000. Thus, this chart suggests the limit of insurance of $1,000,000 is probably way too low and that the buyer should purchase more insurance.

While not discounting outliers is not necessarily incorrect methodologically, and of course, insurance exists to protect against unforeseen losses, it can be misleading, particularly if it's not fully and clearly explained. For example, because outliers are not discounted, insurance brokers using this database are able to suggest to buyers that the impact of loss may be much greater than what their selected limit would cover. However, in this case, if the outlier were discounted, the story would be different. The max loss would be about $550,574, over the client's selected limit of $1,000,000, and the average loss amount in excess would be $550,574, because there would only be one event amount greater than the client's limit. Compare this to the average loss amount of $9,075,287 when an outlier is kept in the analysis. Without including the outliers, the average loss amount is about 15 times less than the average loss amount calculated with outlier events. Therefore, the client's selected limit of $1,000,000, would seem, at first glance, more appropriate to losses experienced by the peer group.

Figure 2

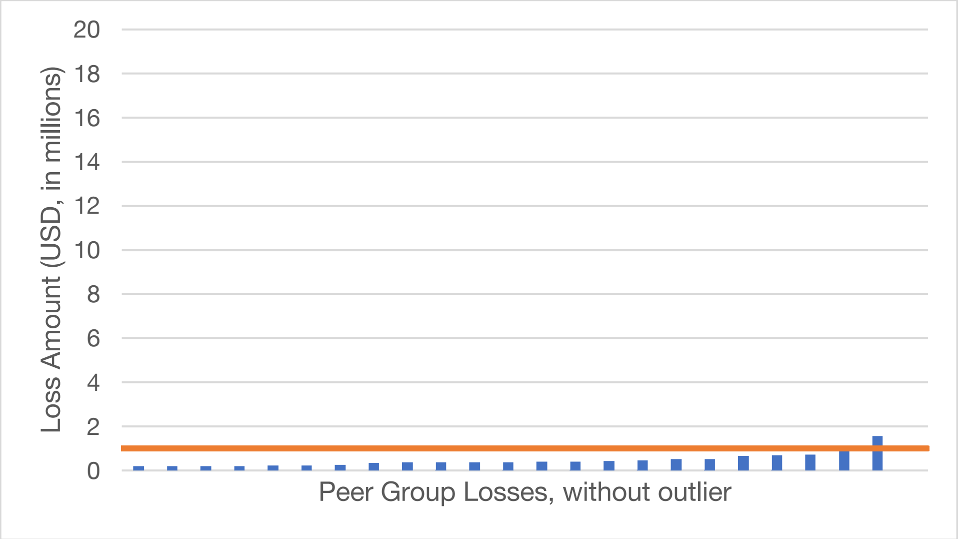


Figure 2. This figure presents the losses experienced by the peer group in Figure 1, without any outliers. The horizontal line is client's selected limit of $1,000,000.

If a user were presented with this visual, as opposed to one with the outlier, the user's selected limit of $1,000,000, even at a quick glance, would look more appropriate to the losses more commonly experienced by this peer group. Not discounting outliers in the model allows brokers to nudge clients toward purchasing more insurance. This result is not a rare occurrence but, to the contrary, consistent with the majority of simulations we ran using the database.[173]

[173] Although we are highlighting how brokers can choose samples and statistical techniques to suit their commercial interest, we recognize that how the data are operationalized is a topic worthy of future focus. For example, sample and statistical techniques may lead to different results. For a thorough analysis of this debate, see Daniel W. Woods & Rainer Böhme, *Systematization of Knowledge: Quantifying Cyber Risk*, 2021 IEEE SYMP. ON SEC. & PRIVACY (forthcoming 2021).

Industry experts note that because many of the big data providers rely on publicly available data, their models tend to recommend higher limits and higher costs for data breach events:

> But a lot of the times, [a data provider uses] . . . all public data. [They] are relying on disclosures by publicly traded companies or companies in regulated industries . . . . So, their numbers are so high. You say, wow, that's really expensive if you have a breach. It doesn't track with what we see day-to-day.[174]

In addition to not discounting outliers, the database presents analytical conclusions based on information collected from multiple, potentially unrelated sources in the same visual, potentially undermining the reliability of decisions based on such representations.

Our own evaluation of the database is consistent with the manner that insurers and brokers we interviewed indicate they use big data. Big data are used to manage uncertainty and nudge buyers toward buying a high limit because the data serves as a legitimizing tool where actuarial data or data specific to the client seeking insurance is spare or missing. As one broker noted, "We manage the uncertainty . . . by showing the peer data. We show them what our models generate[,] [w]hat third-party models like [big data providers] generate."[175] Insurance brokers rely on the database to advocate for the purchase of higher limits, as the graph or chart can "sort of nudge the client into understanding what the recommendation is in respect to limit."[176] Big data are clearly being mobilized to persuade the buyer of insurance: "Absolutely, these graphs, these reports don't do much good if . . . they're not . . . shown to the client."[177] One of the big data aggregators and providers we interviewed commented that one way companies use third-party databases is to "get[] people over the starting line to begin with, just to make the purchase," and to convince midsize and smaller companies that "they actually need to buy the coverage."[178] Using a database that aggregates and presents information about peer group losses can be a "persuasive way to show the kinds of events that happen to companies at a particular industry of a particular size."[179] Insurance brokers explained that these databases legitimize their recommendation that prospective insureds purchase insurance at particular limits:

> And then the client will say, "Well, prove it," and so, he'll show [the big data provider's data], you know. You can put in a healthcare company with such and such revenue, and it'll spit out a chart of, well, okay, here are five

[174] Interview 31, *supra* note 167.

[175] Interview 8, Insurance Broker (on file with author).

[176] Interview 23, *supra* note 136.

[177] Interview 22, *supra* note 131.

[178] Interview 33 Part 1, *supra* note 134.

[179] *Id.* Indeed, no brokers that we interviewed indicated they present big data to prospective buyers to reduce the number of policy limits purchased.

> companies similarly situated to yours, and here are the limits that, you know, they have. And he'll present that, that graph or that chart to help sort of nudge the client into understanding what the recommendation is in respect to limit.[180]

Of course, this reliance on big data providers' data is only effective if the data are accurate and reliable. Similar to our evaluation, security experts have also found that the numbers presented by the data do not align with what they are observing in the industry: "Our numbers are much more conservative, lower than what [the data providers'] numbers come in at. It's what we're seeing in the industry now."[181]

Our research, then, suggests that big data are transforming the underwriting process for insurers and how insurance brokers advise buyers of insurance. This transformation, however, is not necessarily benefiting insureds or enhancing the overall cybersecurity posture of society.

Based not only on our interviews but also on our review of one major cyber insurance-related database's incomplete sources of information, a presentation of information within a database, and the manner in which resulting analysis is used to sell insurance, big data used to make important cyber insurance-related decisions can be unreliable and inaccurate. Big data are used to nudge buyers of insurance toward purchasing more insurance than the limited available data suggest they may actually need. Our analysis reveals that the presentation of big data in the database can intentionally influence a prospective buyer of insurance to purchase higher insurance limits and, therefore, pay a higher insurance premium. Big data in the cyber context create incentives for insurance companies and brokers to sell insurance and enhance profits, and databases like the one we analyzed often serve as a tool to aid that effort, not necessarily for the benefit of consumers.

C. Security Scans and Scoring by Information Security Providers Also May Not Be Reliable and Accurate

As noted earlier, big data provide the fuel for AI and predictive analytics that are penetrating the cyber market. Our research suggests significant problems also exist with this part of the technologization of cyber insurance. Data gathered from external scans and vulnerability scoring by information security providers may seem, at first glance, a more rational way to assess risk and price insurance than prior methods. However, upon closer examination, we conclude that the scanning, scoring, and rating process increasingly relied upon by insurance underwriters to price risk may not be significantly more reliable than older methods.

Insurance industry experts we interviewed indicate that external scans only provide limited information: "Scanning the exterior doesn't tell you very much. It tells you about the web server . . . [b]ut it doesn't really tell you what's going on

[180] Interview 23, *supra* note 136.

[181] Interview 16, *supra* note 146, at 17.

inside of [a potential insured's] network."[182] Others lamented that scoring vendors' scans produce a lot of false positives, i.e., claims that problems exist in the potential insured's cybersecurity profile when actually their profile is fairly secure.[183]

Moreover, because information security providers are running primarily external scans, they cannot precisely identify what is causing the low cybersecurity score or rating.[184] Experts we interviewed believe external scans are not very reliable because, by definition, they cannot capture a full picture of the company's cybersecurity profile:

> The other thing it doesn't pick up on is a lot of clients who outsource their most critical assets—information assets. It's not even them you need to be worried about. It's third-party. Not only third-party, there's fourth-party risk. The cloud's cloud, right? So, none of those [information security providers] are looking at that.[185]

Another expert noted that sometimes companies partner with information security providers that purposely leave "holes" in their security posture that would be picked up by external scans. They might do this to bait would-be cyber attackers to harmless areas of the network in order to catch them. Vendors conducting no-notice external scans and ratings would not realize that is occurring when they issue a low score. The head of a large insurer's cyber division highlights how the security ratings are not reliable:

> [A]n external view of traffic going in and out [is] not telling the whole story. You think about other grades that you might see on a tool like that—for example, if it had a really poor grade on open ports, but the company has a managed services provider for security. Well, the reason for the poor score on open ports might be that they have some honeypots or sinkholes that they have intentionally developed, right, to capture bad actors and watch the bad, threatening traffic that is coming in.[186]

With the exception of insurers dealing with large, high-value clients, the vast majority of insurers do not conduct a follow-up meeting with the prospective insured to discuss more deeply the findings of a security scan. Indeed, multiple insurers and

[182] Interview 12, *supra* note 165, at 7.

[183] *See* Interview 16, *supra* note 146, at 9. ("I see a lot of false positives. It doesn't also pick up on any of the internal side of things that we see causing claims.").

[184] Interviews revealed that many in the insurance field believe the information security providers that conduct "internal" scans are equally unreliable. *See* Interview 31, *supra* note 167 (referring to a company that conducts internal scans and indicating, "I can tell you that their model is nowhere near the point where we would say it's fantastic[,] it's in the early days.").

[185] Interview 16, *supra* note 146, at 9.

[186] Interview 19, Insurance Company Cyber Division Leader, at 8 (on file with author).

brokers repeatedly told us they do not disclose to the buyer of insurance that they are conducting a scan or test and often do not disclose the results of the scan:

> Interviewer: Do you let them know that "Hey, we're going to have BitSight scan your company—"
> Insurer/Underwriter: No.
> Interviewer: Oh, you don't?
> Insurer/Underwriter: No, they're not aware at all that we're using some sort of third-party and getting some sort of rating score from a third-party vendor.[187]

In this respect, insurers miss an opportunity to engage in risk management and loss prevention. Sharing this information concerning vulnerabilities with the prospective insured could potentially improve the cyber hygiene of the organization if they make changes based on the scans. If enough insurers did this, they might gradually "nudge" society as a whole to a more robust cybersecurity posture.

Though some believe the scan-and-score approach has promise, no industry expert we interviewed provided any data suggesting that external scans of a prospective insured's security profile are an accurate proxy for their level of risk or the amount of loss that an insured party might be reasonably expected to suffer in the wake of a successful attack.[188] In fact, some insurers do not even release the information from external security scans to the prospective buyers of insurance:

> So, there are a couple of different vulnerability points that they're testing. But the underwriters are telling me that they won't release the information back to the potential buyer because the data can be distorted. And it's often causing more friction with the potential buyer.[189]

Although security scans exude legitimacy and security, the practical impact on the prospective insured's ability to improve its cybersecurity profile appears to be minimal at best and impossible if they are never told of the scan or results. Moreover, insurers have incentives to sell insurance to gain market share in the growing cyber market, regardless of security scan scores.

The information security providers that provide scans and ratings do not provide continuous or ongoing scans and underwriting throughout the policy period. Neither do they provide recommendations for how the insured can enhance its cybersecurity features.[190] At best, then, the scans are only a snapshot in time, and

[187] Interview 4, *supra* note 135.

[188] As one underwriter and former broker noted, "[T]he external view is a proxy for their overall level of maturity. It's a theory, I wouldn't say it's proven one way or the other yet." Interview 13, Broker & Former Insurance Underwriter, at 6 (on file with author).

[189] Interview 8, *supra* note 175, at 9.

[190] *See* Interview 38, Insurer and Forensics Expert, at 12 (on file with author) (noting that information security providers issuing scores are "definitely not used throughout the policy period for actual monitoring of the portfolio").

they may quickly become irrelevant or even misleading because cyber threats are constantly evolving.

In addition, there appears to be insufficient incentive for the security scanning providers to ensure the accuracy of their scans and analysis:

> BitSight is a company that has no implications if they get it right or wrong, right? They're not going to lose money . . . . [F]irst of all, they need to sell [a] product . . . [and then] a different company, the insurance company, needs to trust what BitSight says so much that they will take huge financial bets based on what BitSight tells them. And, more often than not, this needs to not be just a reflection of what happened in the past. They have to trust BitSight with what is going to happen in the future.[191]

And information security providers are unlikely to challenge, and may not even be aware of, insurers' actuarial teams rejecting their analysis:

> Let's say that you sit on the [insurance] actuary side, and you're like, "You know what, BitSight? I don't know. I hear what you're saying, but I don't trust it. I don't like it." Are you, [as] the BitSight analyst, . . . 100% sure that you're correct? How hard are you going to fight for the insurance company to actually use it? Are you going to jeopardize the contract? Are you going to bang on tables and say that it's an outrage that the actuarial team is dismissing or misusing or misclassifying any of it? [P]robably not, because you need to keep your customer happy.[192]

On top of all the other issues uncovered in our research, it seems that insurers only rarely require prospective insureds to improve their cybersecurity posture as a prerequisite to issuing insurance or even offer meaningful premium discounts for better cyber hygiene. When asked why they do not require changes, insurers noted that the market is so "soft" that prospective buyers can simply go to the next insurance company that will issue insurance without requiring the buyer to make any changes.[193] Moreover, although many insurers we interviewed stated that they rely heavily on technological tools provided by information security providers, there is a lack of transparency in how they implement these tools, creating a sense among some we interviewed that such tools are used arbitrarily.[194]

[191] *Id* at 10.

[192] *Id* at 11.

[193] *See generally* DANIEL WOODS, TYLER MOORE & ANDREW SIMPSON, *The County Fair Cyber Loss Distribution: Drawing Inferences from Insurance Prices*, WORKSHOP ON THE ECON. OF INFO. SECURITY, (2019) (explaining an empirical study showing the cyber insurance premiums fell in absolute terms from 2008–2018, consistent with the suggestion of a soft market).

[194] One expert described the lack of transparency in how security scores are incorporated into underwriting guidelines:

D. Cyber Insurers Role as Quasi-Regulators Is Largely Ineffective—So Far

Cyber insurers tout their ability to play a regulatory role in shaping the behavior of their insureds by preventing, detecting, and responding to cybersecurity risks.[195] Insurers aggressively market and offer a wide variety of pre- and post-breach services to their insureds. However, interviews with insurers and risk managers who purchase cyber insurance reveal that insureds rarely use the pre-breach services offered. Many of our interviewees lamented the low "uptake rate" by SMEs, and more than one risk manager categorically stated fewer than 10 percent of insureds that purchase cyber insurance actually use the vast array of pre-breach services insurers offer that would potentially reduce the insured's potential risk: "The uptake was less than 10 percent in terms of the services that were being offered. But it's a great marketing tool because we're better than the other guys. Look how much free stuff you're getting from us."[196] Reasons provided for not using these pre-breach services include price, not trusting insurer-sponsored services, and underestimating the risk of cybersecurity incidences. Although insurers aggressively market the value of these services at cyber conferences, their ability to nudge insureds' behavior toward greater security in the real world appears to remain low.

Insurers also seem unwilling to require insureds to adopt these pre-breach services as a prerequisite to issuing insurance. Because cyber insurance is such a growing and "soft" market, insurers we interviewed said worried insureds would just seek insurance elsewhere with a less stringent insurer. Thus, although insurers

> And in practice, insurance companies have been buying BitSight for three, four years. I challenge you to find one underwriting guidelines document that explicitly addresses a BitSight or a Security Scorecard finding in how it applies to augmenting price. Not to mention actually declining coverage. So, there is not underwriting guideline anywhere that would say, "If the BitSight score was under 500, decline." "If the BitSight score was under 700, increase price by 20 percent." None of those exist. The BitSight products are used as, let's call it a second opinion portfolio overview analysis tools.

See Interview 38, *supra* note 190, at 12.

[195] The vast majority of insurers and brokers we interviewed indicated they believe insurers "drive some behavioral changes," act as a "motivator to get better coverage," and play a positive regulatory role in the cybersecurity context. Interview 8, *supra* note 175. The following interview excerpt highlights the position of the industry:

> Interviewer: So, what do you think of the insurance company's position as positioning itself as a de facto regulator?
> Insurance Attorney: Well, I think it's a necessity, right? . . . If the federal government can't figure out how to do it, and the states are struggling to do it.

Interview 2A, Insurance Attorney, at 11 (on file with author).

[196] Interview 12, *supra* note 165.

have the *potential* to improve the insured's cybersecurity posture, they appear largely unable to do so, at least in today's cyber insurance "buyer's market."

This reluctance to be rigorous extends to the insurance application itself, where insurers rarely verify or check whether what is listed on the insurance application by SMEs is accurate. Instead, if and when a claim is made, they verify the accuracy of representations made when the victim applied for cyber insurance. If insurers identify inaccuracies, they deny coverage based on misrepresentation.[197]

Thanks again to the soft market—and likely to maximize the efficiency of the sales process—insurers rarely engage in substantive meetings with SME cyber insurance buyers after receiving an application and conducting a security scan. In fact, one chief information security officer described how his company's premiums were *lowered* despite revising their answers to an insurance renewal that showed the company was a higher risk:

> We had a series of like forty questions to answer, you know, "Do you have a written information security plan in place?" Yes. "Do you have an incident response plan?" Yes. "Do you have, you know, annual risk assessments completed?" Yes. So that was the prior year's answer.
>
> When I took a look at it further, you know, it became clear that the person answering those questions just didn't know, but they thought they were supposed to put yes. And we decided, well, we better be as accurate as possible this next time around. And so, we put no, and I warned, you know, our CFO, hey, this is probably going to impact the premium we're charged or the amount of coverage we can get. Somebody's going to ask us questions about it, but I'd rather we're honest on the front end so that we don't jeopardize potential coverage if we ever have a claim. And yeah, they renewed the coverage at a lower premium, and no one ever asked us any question as to why we shifted the answers on that underwriting application.[198]

Thus, although insurers have opportunities to engage in risk management and promote better cybersecurity practices by their prospective insureds and actual customers via (1) closely evaluating application responses, (2) examining the cybersecurity health of the prospective insured, (3) sharing information with the insured regarding the cyber hygiene of the organization based on the security scan evaluation, (4) requiring changes as a prerequisite to issuing insurance or gaining lower premiums, and (5) making sure insureds that do purchase insurance use the

[197] Interview A2, Insurance Expert & Attorney (on file with author) (discussing how insurers rely on post-claim underwriting and misrepresentation doctrine).

[198] Interview 20, Chief Information Security Officer (on file with author).

insurers' pre-breach services to prevent and detect risks, our research indicates most insurers seldom do any of these things.[199]

Perhaps even more troubling, our research clearly indicates that large and small/medium organizations seeking cyber insurance are not treated equally by insurers: "Not all customers are treated the same way, and so we are using third-party data [from big data providers and information security providers] to help better distinguish good customers from bad customers and tie that directly to our rating."[200] Because insurers are eager to expand into the cyber market, insurers underwrite SMEs based on the insurance application and sometimes an external security scan rating from one of their information security partners. Insurers rarely meet with and engage in a deep discussion of the SME's specific cybersecurity posture. Concerns over efficiency and cost-containment rather than the perceived preferences of the SME's themselves shape the way in which cyber insurers determine whether to actually meet with the prospective buyer about their cybersecurity health:

> In the SME space, it's more reliant on that third-party external view. You almost would never get the sixty-minute call. And the application may have some additional information. But the SMEs are really looking for an ease of transaction. The [insurance] companies that are successful are really minimizing the amount of information they are requesting. From our standpoint, we work with an insurtech that bakes in that external analysis into their underwriting.[201]

On the positive side, insurers and risk managers we interviewed indicate that insureds regularly use insurers' post-breach services. Thus, it was quite common for insureds to rely on the insurers' recommended panel of lawyers, forensics, and client management specialists. However, since these services occur, by definition, after the breach, they do not prevent successful attacks and are unlikely to improve our society's overall cybersecurity posture. The uptake of post-breach services does, however, suggest that cyber insurers actually can have a positive "regulatory" impact on insureds with the right incentive structure to change behavior.

E. The Same Information Quality and Reliability Problems Also Affect State Regulators

Our research indicates that the ineffectiveness of insurers as regulators to date is compounded by the impact of information quality and reliability issues on the actual state and federal regulators themselves.

[199] *See generally* Daniel W. Woods & Tyler Moore, *Does Insurance Have a Future in Governing Cybersecurity?,* 18 IEEE SEC. & PRIV. 21, 21 (2020) (suggesting insurers may have problems in governing the cybersecurity practices of organizations).

[200] Interview 35, *supra* note 133.

[201] Interview 13, *supra* note 188.

First, although AI and predictive analytics are being used by cyber insurers, one information security provider that provides the AI tools for insurers indicates that such tools are not being incorporated into the filings with state regulators.[202] The way these antiquated regulations are drafted, the companies must include traditional actuarial methodologies in their required reports, regardless of how they actually price and underwrite cyber insurance.

Even more troubling, this same flawed data may be shaping the content and meaning of actual legal regulations that are intended to regulate cyber insurers.[203] For example, regulators and rating agencies are working with the very same information that security providers and insurers use to develop their own rating, risk, and monitoring systems to regulate insurance companies:

> We work with carriers. We work with regulators and rating agencies like Standard & Poor's. For example, Standard & Poor's, what they've done is they use some of [our] analytics, and they've embedded them into a report that any companies and users can go buy about themselves. And it will have a variety of things and benchmarks and comparisons.
>
> . . . .
>
> . . . . [W]e've worked with state regulators to come up with frameworks for how they should be evaluating cyber exposures . . . .
>
> . . . .
>
> And so, a lot of times what we've been doing is trying to couple our analytics with their processes.
>
> . . . .

[202] As one information security provider noted, insurers are actively incorporating AI:

> Interviewer: Your sense is that the cyber insurers are actively using AI in ways of evaluating risk and pricing risk?
> Information security provider: They're working with us. And they're using our models, but they still have state regulations. So, they're filing their actuarial model. A traditional actuarial model. And according to the regulations and according to the state filings, that's how they have to price the business. But people are working with us to maybe apply some of the outputs of our model and input it into their rating model.

Interview 32, *supra* note 142.

[203] *See generally* Shauhin Talesh, *A New Institutional Theory of Insurance*, 5 U.C. IRVINE L. REV. 617, (2015) (laying out a theoretical framework for explaining how insurers influence the meaning of law and compliance).

> . . . .[T]he regulators we work with are state insurance regulator or bodies like Lloyd's. So, the people that are overseeing the insurance companies and the financial services companies, those are the regulators we're primarily focused on . . . . [I]f you went to the NAIC, the National Association of Insurance Commissioners Conference, they even had a mini-pitch session for insurance tech companies. So, I'd say the regulators are definitely interested and integral to all the innovation you see in the insurance space in general, as well as for cyber.[204]

To the extent these predictive analytic models developed by information security providers are built upon inaccurate, unreliable, and incomplete data (as our findings suggest), state regulators and private standard-setting organizations are adopting and legitimizing a flawed model into its regulatory framework. Moving forward, there needs to be more transparency concerning the technology tools insurers are actively using and more scrutiny by state regulators of the accuracy and reliability of these tools.

To summarize, although technology and big data offer some promise, the intersection of insurance and technology is problematic. Big data in this sector is limited, inaccurate, and misleading. Insurers use technology and security tools to scan and evaluate the cyber hygiene of a prospective insured but do not make improving their cybersecurity posture a prerequisite to obtaining coverage. Moreover, insurers are fighting aggressively for market share. Because of a desire to secure as many insureds as possible, insurers' ability to change or influence insured behavior is weakened. Insureds who do have very strong security protocols do not necessarily reap the benefits of such good behavior in the form of lower premiums. Although insurance companies offer a series of security programs and tools that, in theory, could help an insured protect itself against being breached, most insureds do not take advantage of these "pre-breach" services, even when offered free of charge.

Thus, our research regrettably indicates that, at least for now, cyber insurers are not significantly improving the cybersecurity posture of most insureds. And once insurance is issued, most insurers do not monitor the insured's cyber hygiene. Even though insurers tout their role as de facto regulators of organizational behavior, their impact so far appears to be marginal in terms of heightening the insured's cybersecurity readiness.

V. A POSSIBLE PATHWAY FORWARD: FULLY INTEGRATING INSURANCE AND TECHNOLOGY

Although the intersection of insurance and technology is problematic, none of the above suggests that cyber insurers cannot play a meaningful role in improving their insureds' cybersecurity posture and, eventually, that of society as a whole. Big data, AI, and new technologies are revolutionizing the delivery and practice of

[204] Interview 32, *supra* note 142.

insurance, and there is no turning back. Despite the challenges articulated in Part IV, we suggest in this Part that insurtech can, in theory, be a part of the solution and can help increase organizations' cybersecurity and insurers' ability to play a positive regulatory role.

To do so, however, insurers must turn their focus from only using such technologies and data to increase efficiency, speed, and profit to also using them to incentivize—and perhaps require—better cyber hygiene by their insureds. The solution, we argue, lies in addressing some of the problems identified in Part IV and altering how cyber insurance is negotiated and delivered. To be clear, we are not suggesting that an insurance-company-as-regulator model will work. Rather, we are saying that if it is going to work, insurers will need to address some of the problems that we identified in Part IV.

Based on our research and analysis, we argue that insurtech companies should: (1) engage in continuous evaluation and underwriting throughout the life of cyber insurance policies, (2) make insurance premium pricing contingent on reliable evidence of good cybersecurity practices (i.e., reward good behavior with reduced premiums), (3) when necessary, require prospective insureds to make changes to improve their cybersecurity posture as a prerequisite to issuing insurance, and (4) engage in dynamic risk management and loss control throughout the policy period to reduce insureds' risk of loss.

The potential benefits to a widespread adoption of such recommendations are not theoretical. Coalition, Inc. and At-Bay are two companies that, unlike traditional insurance companies that contract with third-party vendors to provide background security analysis of prospective insureds, embed technology and security within the insurance company itself (full integration) and have incorporated some of what we recommend here with modest success.[205] Founded in the last decade by individuals with security and technology backgrounds,[206] these fully integrated insurtech companies combine comprehensive insurance and proactive cybersecurity tools to

[205] For background on how Coalition operates, see *Coalition Enters Excess Cyber Insurance Market*, CISION (July 22, 2020), https://www.prnewswire.com/news-releases/coalition-enters-excess-cyber-insurance-market-301097844.html [https://perma.cc/62D8-9CV5] [hereinafter *Coalition Enters*]; *Coalition—Cyber Risk Solved*, COALITION, https://www.coalitioninc.com/ [https://perma.cc/R2ZM-FG7P] (last visited Jan. 25, 2021). For background on how At-Bay operates, see *Insurance for the Digital Age*, AT BAY, https://www.at-bay.com/ [https://perma.cc/37CJ-ZUQY] (last visited Jan. 25, 2020).

[206] One insurance broker that deals directly with Coalition describes how they operate:

> They basically are a tech company with some insurance people involved. So, Swiss Re is there and a gentleman that used to be the head of Aon's international privacy security liability practice helped form this startup. And they had venture capital to help form this startup. And they hired tech people to evaluate the risk using these external scans. Now they feel very confident about the scans that they're doing. And they're using it to basically decide "Yay or nay, are we going to write this risk?" And then price it based upon the controls that they see.

Interview 8, *supra* note 175, at 9.

underwrite exposure and help businesses manage and mitigate cyber risk.[207] These companies primarily focus on offering insurance to small and medium-sized companies. They are, however, expanding and now offer insurance in all fifty states.[208]

Recognizing that cyber threats constantly evolve, these companies focus on using security and technology to evaluate the cyber hygiene of the company and issue a quote within three to five minutes of receiving a company's information.[209] Upon receiving basic information filled out online, these companies rely on technical and domain expertise and have built proprietary and automated tools that conduct external scans of the dark web, internet, and relevant IP addresses. Once they identify the risks and assign a risk score, they use an automated machine that relies on predictive analytics and modeling to issue an insurance quote within particular parameters.[210] If the scan does not trigger any flags or warnings, an insurance quote is generated. If the scan does trigger a warning, the application is referred to an underwriter to make a final determination.[211] Whereas traditional

[207] Both insurtech companies are financed by leading global insurers because one cannot sell insurance without being a licensed insurance company. Coalition is supported by Swiss Re Corporate Solutions, Lloyd's of London, and Argo Group. *Coalition Enters*, *supra* note 205. At-Bay is supported by Munich Re. Charlie Wood, *Munich Re-backed At-Bay raises $34mn in Series B round,* REINSURANCE NEWS (Feb. 24, 2020) https://www.reinsurancene.ws/munich-re-backed-at-bay-raises-34mn-in-series-b-round/ [https://perma.cc/C2AQ-9LKA].

[208] *Id.* There are also differences between Coalition and At-Bay. The key differences are that At-Bay does its own underwriting and claims management, whereas Coalition has Swiss Re handle its underwriting. At-Bay has hired an entire team of underwriters and handles underwriting and claims decisions internally. In general, Coalition has the authority to make decisions up to about $200 million, whereas At-Bay has authority to make decisions up to $2 billion. Thus, Coalition tends to be focused on small and medium businesses, whereas At-Bay also focuses on larger companies. Interview 38, *supra* note 190, at 17–18.

[209] Interview A2, *supra* note 197 ("It's an [insurance application] form and a quote, and they ask you all the questions they need to ask you in four minutes.").

[210] Interview 11, Underwriter & Broker (on file with author).

[211] At-Bay indicates their model relies on asset discovery and automation:

> [W]e're collecting information ourselves by scanning the company. We also collect threat intelligence from a bunch of resources out there. So, honestly, there are two steps to it. There's the asset discovery part. So, the company doesn't give you a list of all of their machines and all of their IP and all of their inventory. So, you kind of have to discover that yourself. So, the first part is discovering their assets, and the second part is understanding to what extent those assets or configurations are vulnerable to attacks. That's the first thing that we do that is very different. And then all that information flows into a machine that makes all of its decisions by itself. So, we've removed the human from the underwriting decision process unless there's either a red flag or the risk is big. [T]here are parameters . . . .

Interview 38, *supra* note 190, at 5–6.

insurers measure a company's risk based on their past behavior, these companies measure a company's risk based on what they can find on the web and dark web and, in doing so, analyze a company's future risk, as explained by one of our interviewees: "Instead of underwriting for last year's risks, can you underwrite for this year's risks? And how do you do that if those risks keep on changing? The answer is real-time underwriting and real-time risk management."[212]

Under the traditional model, once the insured agrees to an insurance contract, the insured's coverage is locked in for one year regardless of whether the risk changes. But fully integrated insurtech companies instead conduct continuous underwriting and "a more involved, active risk management and monitoring of the security of [their] insureds throughout the year."[213] Whereas most mainstream cyber insurers offer pre-breach services that policyholders only use 10 percent of the time, fully integrated insurtech companies embed pre-breach monitoring security features into the insurance itself and significantly increase adoption by insureds. If they identify that a threat is imminent, they alert the company and work with the company to avoid the threat. Such insurers offer risk transfer and risk management simultaneously.

Fully integrated insurtech companies such as At-Bay also take the unique step of scanning and evaluating the cyber hygiene of the insured throughout the length of the insurance policy. This form of continuous underwriting and risk management is unique in the cyber context and seems to offer a more robust and effective form of "regulatory nudge" by the insurer toward improving the cyber hygiene of its insured:

> And the last part is, once a company is in our portfolio, we use the exact same underwriting engine that we've used to provide a quote in the beginning of the policy period. We run that engine basically once a month on every one of our policyholders.
>
> And if that engine now shoots up an alert, then we have a security team who would reach out to the insured and say basically, "Look, we already sold you a policy. We're not trying to get any more money from you. We're on the hook to pay most of it. But you're also on the hook. We're seeing this new attack come in, and we can see that you're vulnerable. Here are the details of specifically what the attack is. Here's your specific machine that's vulnerable. Our team is here at your disposal to help you fix it."

[212] *Id.* One insurance expert highlighted how fully integrated insurers flip the business model: "It's interesting the way they're doing it, it's not 'we're a traditional insurance company. We've been underwriting for hundreds of years; we know how to underwrite this.' 'No, we're a tech company. We have no background in insurance, but using our technology, we can identify risks that these other insurance companies will never find.'" Interview A2, *supra* note 197.

[213] Interview 38, *supra* note 190, at 2.

> And just to give you a few examples, over the last couple months, . . . [w]e ha[d] almost two dozen companies that had a Citrix installation that was vulnerable to a ransomware campaign that was exploiting that vulnerability . . . . We had a Palo Alto Networks issue that we helped solve. We helped solve RDP ports issues with, whatever, BlueKeep and some of the other issues that happen with RDP.
>
> [W]e're just kind of going one by one. And whenever there's a new alert or a new critical vulnerability, it flows from the research team to the model. And then the model runs on all of our portfolio [of clients] and spits out alerts. And then the security team just helps companies fix the issue.[214]

"Real-time" monitoring increases the likelihood that the insured will maintain a healthy cybersecurity environment because the insurance company is continuously monitoring and checking for threat vectors. Insurtech companies make using their risk management services a requirement under the policy and assure their clients actually use the tools. As one leading insurtech company official noted, "Post-bind pre-breach [is] built into everything we do."[215]

Moreover, unlike other insurers, insurtech companies tie premium price to existing risk and loss control measures and, in particular, reward the insured with lower premiums for heightened security:

> Interviewer: Have companies said, "Sure, I will make these security changes that you suggest. And please give me the improved price." Has that experience occurred?
> Interviewee: Yes, it happens quite often. It happens ever more often. . . . [F]or example, the other recommendation that we ask them to do is we ask them to add a security email gateway like a Barracuda or a Mimecast or a Proofpoint. And when they do that, we give them significantly broader coverage. We have these every day. We have a few coming back and saying, "We've added something. We've improved something. We changed our configuration. Can we please get the better terms?" And by the way, most of the time, they do it before they buy the insurance. So, they get the first quote from us. They make the fixes. We improve the offer, and then they bind the insurance.[216]

Rewarding the insured for good behavior is built on a very basic concept: "[T]he better the scan comes out, the better your premium will be."[217] Despite the soft market where insurers are trying to acquire as much business as possible and

[214] *Id* at 7.
[215] *Id* at 13.
[216] *Id* at 15.
[217] Interview 1, Insurer Underwriter (on file with author).

are resistant to nudging insureds toward making changes to their cybersecurity posture,[218] fully integrated insurtech companies suggest such an approach is possible. In theory, this makes insureds safer from risks, decreases the chances that the consumer data that those organizations maintain will be exposed, and allows insurers to play a more substantive rather than symbolic regulatory role, ultimately to the benefit of society overall.

Unlike the majority of traditional insurance companies we interviewed, the fully integrated insurtech companies are not afraid to require an insured to make changes as a prerequisite to coverage. For example, remote desktop protocol ports (RDP) account for almost 25 percent of ransomware losses insurers paid out on in 2018 and 2019. As such, At-Bay requires that insureds have "closed" RDP ports to reduce the chance of malfeasance by hackers. At-Bay tells us they currently have 0 percent of open RDP ports among its insureds, "[b]ecause when you come to us and ask for insurance, if you have an open RDP port, we will say 'No,' unless you fix it."[219] This regulatory nudge by the insurer should result in fewer claims for the insurer, fewer breaches for the insured (often a business), and reduced harm to consumers.[220] During COVID-19, as the vast majority of corporate employees worked remotely from home, insurtech companies noticed via their monitoring that a number of companies opened up unprotected RDP ports. They notified the businesses of the vulnerability and instructed them on how to fix it. Engaged in ongoing monitoring and risk management of their insureds, this insurer is able to avert risks that others in the cyber insurance ecosystem could not:

> I would say about half of them fixed it within 24 hours. And then probably 20 percent more, it took a week to two weeks to fix it. A few of them tried to argue why it's not an issue. With most of them we were able to figure it out. And some of them are either refusing or did not answer the phone. But that was the minority. So yeah, we do have maybe three of them open right now, which we're frustrated by. Because it happened in the middle of the policy, we're not going to pull the policy away, but we haven't given up on helping them fix it. We do think it matters.[221]

We do not mean to suggest that fully integrated insurtech models are foolproof, nor do we endorse any particular insurance provider. However, given the limited government oversight and the need to motivate insurers to regulate in a more effective manner, the continuous underwriting and risk management approaches being deployed by fully integrated insurtech companies throughout the entire insurance policy period addresses some of the challenges highlighted in Part IV and more appropriately align the incentives between insurers and insureds. Industry

[218] *See supra* Part IV.

[219] Interview 38, *supra* note 190.

[220] "[O]ur peers experience on average about 25 percent of their losses coming from RDP ports. For us, in 2018 and 2019 it was zero percent. And our losses have been lower, and our frequency is less than half that of the industry." *Id.*

[221] *Id.*

experts we interviewed indicate that Coalition and At-Bay's emphasis on real-time underwriting and risk management reflects the future of insurance:

> [T]hey're kind of doing real-time underwriting. Once [a client] become[s] an insured, then they take them under their wing, and they protect them as much as they can . . . . [This is] the future of cyber insurance . . . . [I]t's going to be managed security services with insurance attached to it. I really believe that's what's going to happen.[222]

If fully integrated insurtech models are successful, insurers may manage and reduce uncertainty in the cyber market better and improve their position as a *de facto* regulator of the insured's cybersecurity.[223] At a minimum, we view these new approaches as trying to address some of the deficiencies we identified in Part IV.

We also believe there is a role for government to play. First, many of those we interviewed believe that the government should work with the insurance industry to require them to share anonymized data using more standardized terminology. This would increase transparency both for consumers and regulators on how data are used, as well as reducing some of the information access disparities between larger and smaller insureds and insurers. Second, the government should develop public-private partnerships between private industry, government, and researchers to enable two-way collaboration and cooperation to identify, mitigate, and disrupt cyberattacks.[224] Third, rather than organizations trying to comply with fifty different state privacy laws and notification statutes, the federal government should create a federal privacy law to reduce the fragmented legal framework concerning privacy law. Finally, the federal government should consider creating a financial backstop for the cyber insurance ecosystem in the event of a catastrophic cyberattack.[225]

[222] Interview 12, *supra* note 165, at 5.

[223] As one industry leader noted, "[N]othing we do is better than anything else that is out there already in the security industry. The one thing that we're doing which is really difficult is integrating it. Like actually injecting it into the DNA of the insurance company. Not putting it as a patch on top." Interview 38, *supra* note 190, at 12.

[224] An early form of this two-way collaboration exists. The National Cyber-Forensics and Training Alliance (NCFTA) is a nonprofit organization existing somewhere between private industry, government, and academia for the purpose of providing a neutral, trust environment that enables two-way collaboration and cooperation to identify, mitigate, and disrupt cybercrime. Financial institutions, federal and state law enforcement, and other entities attempt to communicate, collaborate, and disrupt and dismantle cyber threats. *See The National Cyber-Forensics and Training Alliance*, NCTFA, http://ncfta.net [https://perma.cc/7NXC-8D8J] (last visited Jan. 27, 2021).

[225] For a legislative proposal on a government-led financial backstop program for catastrophic cyber risks, see Bryan Cunningham & Shauhin A. Talesh, *Uncle Sam RE: Improving Cyber Hygiene and Increasing Confidence in the Cyber Insurance Ecosystem via Government Backstopping*, UCONN. INS. L. J. (forthcoming 2021).

CONCLUSION

No business likes government regulation, but most like successful cyberattacks against them even less. In the absence of comprehensive cybersecurity regulation in the United States, we took a deep-dive look at the potential role of cybersecurity insurers as *de facto* regulators. How is that working out so far? Not well, as we document above.

More broadly, volumes have been written over the last decade about the transformative role of big data, AI, and emerging technologies in every aspect of our economy and, indeed, our lives. But will these transformations balance out for our good or work toward our detriment—whether as individuals, companies, economies, or state and national governments? What is the ground truth about how these revolutionary technologies actually affect us all in the real world?

Much to our surprise, we found that very little has been written about these real-world effects on significant parts of our society, economy, or security. Using a variety of empirical methods, to our knowledge, this Article provides one of the first close looks at the real effects of these technologies—in this case, on the cyber insurance ecosystem.

Have these new technologies significantly enhanced our collective cybersecurity? Have they had a meaningful positive effect on insureds' cybersecurity postures?

Our research indicates that, despite the theoretical promise of cyber insurers being able to significantly enhance their insureds' cybersecurity, the promise remains just that: theoretical. As discussed in detail above, the reasons for this failure include: a "soft" insurance market in which insurers hotly compete for market share, the resulting reluctance on the part of cyber insurers either to reward good cyber citizens with lower premiums or to punish those insureds unwilling or unable to improve their cybersecurity posture—whether through denial of coverage or higher premiums, the unreliability of big data and information security provider security scans that insurers and brokers heavily rely on, and the frequent use of emerging technologies to improve policy sales and increase profit margins rather than to incentivize good cyber citizenship. Although mainstream cyber insurers are turning to big data and technology as mechanisms to manage uncertainty in the cyber market, such models are not fully integrated into the underwriting and risk management processes.

But there is hope.

The building blocks are in place for cyber insurers to transform their role into one of improving cybersecurity across companies and industry sectors. Building on our recommendations in Part V, we believe that the promise of cyber insurers as *de facto* regulators may gradually be realized if they address the problems identified in this Article. These technology tools need to be—and can be—reprioritized to focus on consumer and organizational safety and security, as opposed to greater efficiency and cost containment. Finally, we hope this deep dive into the real-world effects of big data, AI, and emerging technologies on the cyber insurance ecosystem will inspire similar studies in other areas of our economy and society. We encourage policymakers and scholars to focus their attention on ways to improve data transparency and protection—as well as algorithmic accountability and justice in society.