Penn State Law Review

Volume 123 | Issue 3 Article 3

6-1-2019

Reining in Commercial Exploitation of Consumer Data

Max N. Helveston

Reining in Commercial Exploitation of Consumer Data

Max N. Helveston*

ABTRACT

The collection and use of consumer data by commercial entities has quickly transitioned from being an obscure topic to a headlining issue in leading media outlets. The burgeoning societal awareness of how digital devices are collecting and transmitting data about individuals has led to growing concerns about how this information is being used, stored, and sold. Legal scholars have identified insurance as one of the market sectors where commercial use of individuals' data could be particularly harmful to consumers. They have argued that, if left unrestricted, insurers would use Big Data analytics in ways that would decrease marginalized populations' access to insurance, limit individual liberties, and allow insurers to shirk their contractual obligations.

Working from the assumption that these concerns are valid, this Article considers whether existing laws are sufficient to prevent these abuses and provides an account of where further protections are needed. It argues that the primary laws targeted at restricting companies' purchase and use of personal data—the Fair Credit Reporting Act, the California Consumer Privacy Act, and the Vermont Data Broker Act—may prevent certain problematic behaviors, but will not deter others. Additional state action will be necessary to protect consumers from exclusionary advertising practices, unfair underwriting rules, and bad faith claims handling behaviors.

*Max Helveston is the Associate Dean of Academic Affairs and Associate Professor of Law, at DePaul University College of Law. The author would like to express his sincere gratitude to the executive board of the Penn State Law Review for organizing the symposium and for all of the work that went into editing this piece.

Table of Contents

I. INTRODUCTION

One of the hottest topics in recent years has been society's growing recognition of the enormous market for consumers' personal information and how current laws provide individuals with almost no control over who records, purchases, and sells their data.[1] With news of major data security breaches and privacy policy lapses in the headlines regularly,[2] it is not

1. *See, e.g.*, Emily Glazer et al., *Facebook to Banks: Give Us Your Data, We'll Give You Our Users*, WALL ST. J. (Aug. 6, 2018), https://on.wsj.com/2Oh1p2Q; Khadeeja Safdar, *On Hold for 45 Minutes? It Might Be Your Secret Customer Score*, WALL ST. J. (Nov. 1, 2018) https://on.wsj.com/2SFhK46; Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://nyti.ms/2SFm9DE; *How to think about data in 2019*, THE ECONOMIST (Dec. 22, 2018), https://econ.st/2EGaTUk; *see also* Bill Davidow, *Redlining for the 21st Century*, ATLANTIC (Mar. 5, 2014), https://bit.ly/2H3IDK6 (describing prohibitions against redlining and how Big Data could lead to unfair discrimination in the commercial sector).

2. *See, e.g.*, Raymond Zhong, *Quora, the Q. and A. Site, Says Data Breach Affected 100 Million Users*, N.Y. TIMES (Dec. 4, 2018), https://nyti.ms/2AUpAyO; Mike Isaac &

surprising that individuals have begun to look to the government to enact laws that will protect their interests.[3] While the United States federal government has not been able to pass a comprehensive consumer privacy law like the European Union's General Data Protection Regulation, state legislatures have begun to enact consumer privacy statutes.[4]

Legal scholars have identified a variety of ways in which insufficient protection for consumer privacy will harm consumers.[5] Some have identified insurance as one of the market sectors where businesses' use of individuals' data poses a particularly large threat to consumer welfare.[6] They have argued that, if left unrestricted, insurers could use Big Data analytics in ways that would decrease marginalized populations' access to insurance, limit individual liberties, and allow insurers to shirk their contractual obligations.[7]

This Article provides an account of whether the data protection laws that are currently in effect are sufficient to address these insurance-related problems and to proscribe solutions for regulatory gaps. Part I discusses the threats to consumer welfare that will manifest if the law allows insurance companies' unfettered access to consumer data and permits them to integrate analytics throughout their business operations.[8] Part II analyzes some of the primary laws that regulate commercial use of consumer data—the Fair Credit Reporting Act, the California Consumer Privacy Act, and the Vermont Data Broker Act—and discusses each law's applicability to insurers.[9] Part III concludes by discussing whether these laws are sufficient to deter insurers from engaging in problematic

Natasha Singer, *Facebook Says Bug Opened Access to Private Photos*, N.Y. TIMES (Dec. 14, 2018), https://nyti.ms/2rD7Rb6.

3. *See* David Meyer, *In the Wake of GDPR, Will the U.S. Embrace Data Privacy?*, FORTUNE (Nov. 29, 2018), https://bit.ly/2AIIGrV; *Americans Say, "Bring on the Data Privacy Regulations!"*, EMARKETER (May 21, 2018), https://bit.ly/2LmLG5z.

4. *See infra* Part II.

5. *See, e.g.*, Kate Crawford & Jason Schultz, *Big Data and Due Process: Towards a Framework To Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 96–109 (2014); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 7 (2014); Tal Z. Zarsky, *Understanding Discrimination in the Scored Society*, 89 WASH. L. REV. 1375, 1378–79 (2014); Amy J. Schmitz, *Secret Consumer Scores and Segmentations: Separating "Haves" from "Have-Nots,"* 2014 MICH. ST. L. REV. 1411, 1451–52 (2014).

6. *See* Max N. Helveston, *Consumer Protection in the Age of Big Data*, 93 WASH. U. L. REV. 859, 859 (2016) [hereinafter Helveston, *Consumer Protection*]; Rick Swedloff, *Risk Classification's Big Data (R)evolution*, 21 CONN. INS. L.J. 339, 339 (2014–2015); Peter Siegelman, *Information & Equilibrium in Insurance Markets with Big Data*, 21 CONN. INS. L.J. 317, 329 (2014–2015).

7. *See* Helveston, *Consumer Protection*, *supra* note 6, at 859; Swedloff, *supra* note 6, at 339; Siegelman, *supra* note 6, at 329.

8. *See infra* Part I.

9. *See infra* Part II.

behaviors and suggests specific regulatory approaches that should be used to address any shortfalls.[10]

II. PART 1 – BIG DATA ANALYTICS, INSURERS, AND THE THREAT TO CONSUMERS

Legal scholars have identified legal and societal problems that are likely to manifest due to the widespread availability of consumers' personal data and rapid advancements in the analytic sophistication of commercial entities.[11] While some articles have looked at how these changes will affect consumers' generally, others have focused on specific sectors. There have been a handful of articles looking at the problems that could result from use of consumer analytics in the personal insurance market.[12]

It is not surprising that the academics working in this field have expressed significantly different views about the type of risks posed by Big Data-informed insurers and the extent to which additional regulation is needed to protect consumers. Despite this lack of consensus, the literature has done a good job of identifying the potential ways that insurers' use of individuals' data could imperil consumer welfare. This Part will provide an overview of these threats in two steps. First, it will discuss the three segments of insurers' operations that could change with increased use of analytics. Second, it will review the different types of harms that consumers could suffer.

A. How Big Data Analytics Could Change Insurers' Operations

It is worth noting that the threats to consumer welfare posed by the integration of Big Data into the insurance industry have the potential to be more substantial than they are in other market sectors. Not only will the

10. *See infra* Part III.

11. *See* Charlotte A. Tschider, *Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age*, 96 DENV. L. REV. 87, 130–31 (2018); Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data*: *A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 63–65 (2012) ("Data has become the raw material of production, a new source of immense economic and social value."); Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 248 (2013) (discussing business benefits of big data); Crawford & Schultz, *supra* note_5, at 96–109 (discussing privacy harms associated with the use of predictive analytics); Citron & Pasquale, *supra* note 5, at 17–18; Zarsky, *supra* note 5, at 1375; Schmitz, *supra* note 5, at 1411; Ed Mierzwinski & Jeff Chester, *Selling Consumers Not Lists: The New World of Digital Decision-Making and the Role of the Fair Credit Reporting Act*, 46 SUFFOLK U. L. REV. 845, 866–67 (2013); Max N. Helveston, *Regulating Digital Markets*, 13 N.Y.U. J.L. & BUS. 33, 33 (2016).

12. *See* Helveston, *Consumer Protection*, *supra* note 6, at 859; Swedloff, *supra* note 6, at 339; Siegelman, *supra* note 6, at 317.

use of Big Data analytics result in the selective advertising and marketing behaviors that have been identified as a problem for all business entities,[13] but the unique nature of the insurance relationship means that there will be additional dangers. Unlike the typical consumer transaction, which involves an instantaneous or near-instantaneous exchange, the contracts between insurance companies and consumers necessarily create a long-term contractual relationship between the parties and incentivize insurers to be selective about which individuals they sell coverage to. Further, insurance contracts invest insurance companies with substantial discretion about when and how they need to perform. Finally, pricing discrimination is common and non-controversial in insurance markets, so long as it stays within statutory and regulatory boundaries. This unique constellation of characteristics creates novel opportunities—specifically in underwriting and claims handling—for insurers to engage in unfair Big Data-related practices.[14]

1. Marketing

Practically anybody who has watched television, engaged with online media, or browsed the web can attest to the fact that insurance companies spend a substantial amount each year on advertising and marketing their products to consumers.[15] Commercials for automotive, homeowner's, and other personal lines of coverage have become prevalent across digital media platforms. These advertisements use mascots (e.g., the GEICO gecko, Flo the Progressive agent) and slogans (e.g., "Like a good neighbor, State Farm is There") designed to instill potential customers with a sense that the insurer will act in the policyholder's best interest and build brand affiliation.[16]

The growth of the digital world and the increasing amount of time that individuals spend online have begun to revolutionize how businesses approach marketing. Insurers, like other businesses, have started to look at

13. *See, e.g.*, FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? 8–9 (Jan. 2016), https://bit.ly/1n52gG6 [hereinafter FTC, BIG DATA]; PETER CORBETT ET AL., IBM INST. FOR BUS. VALUE, ANALYTICS: THE REAL-WORLD USE OF BIG DATA IN INSURANCE 3–7 (May 2013), https://bit.ly/2V2t4HN (describing how advanced analytics could be incorporated into insurers' marketing, underwriting, claims management, and other practices); STACKIQ, CAPITALIZING ON BIG DATA ANALYTICS FOR THE INSURANCE INDUSTRY 3–4 (2012), https://bit.ly/2GXx2ML (same).

14. *See* Helveston, *Consumer Protection*, *supra* note 6, at 887–88.

15. *See* Craig Davis, *Why Do Insurance Companies Advertise So Much?,* THE CONTENT STRATEGIST (Feb. 6., 2017), https://bit.ly/2ViCeVB; Jessica McGregor & Megan Sutela, *How Advertising Spend, Underwriting Results Relate to Auto Insurers' New Business Yield: J.D. Power*, INS. J. (June 19, 2017), https://bit.ly/2Wquv43.

16. JAY M. FEINMAN, DELAY, DENY, DEFEND: WHY INSURANCE COMPANIES DON'T PAY CLAIMS AND WHAT YOU CAN DO ABOUT IT 53 (Penguin Group 2010).

how predictive analytics could inform and improve the ways they reach out to potential consumers.[17] Not only are they keen on finding ways to ensure that potential customers get advertisements that are optimally tailored for the recipient, but there is interest in making sure that their ads are being delivered to the specific communities the insurer wishes to target.[18]

The nature of the insurance agreement gives insurers an even greater incentive to engage in marketing activities that focus on certain groups and excludes others than with other commercial entities. Whereas vendors engaged in the sale of simple goods or services can easily determine how much it will cost them to perform their end of a deal, insurance companies cannot. Instead, the cost of performance for any given policy will depend on whether the policyholder suffers fortuitous covered losses. This dynamic creates a large incentive for insurers to do what they can to avoid signing deals with consumers that are likely to suffer large losses or who are difficult to predict accurately.[19] In the context of marketing and advertising, this would mean using targeted advertising practices that exclude individuals with characteristics that indicate high risk or volatility.

While this type of screening might seem unobjectionable—at first glance, it seems nearly identical to the screening that insurers engage in when underwriting—there are unique harms associated with using selective advertising practices to limit the applicant pool. First, doing so could allow insurers to effectively undermine existing laws and regulations that prohibit certain underwriting practices.[20] Second, it may be more difficult for potential policing entities (e.g., plaintiff's attorneys, insurance regulators) to take action against insurers that use selective marketing to prevent certain populations from applying for insurance than it would be if the insurers were denying these groups through the underwriting process.[21]

2. Underwriting

For as long as insurance arrangements have existed, insuring entities have used data to inform their underwriting decisions. Indeed, insurer solvency is largely dependent upon their ability to analyze information about their applicants and make prudent decisions about the rate (if any)

17. *See* CHARLES NYCE, AM. INST. FOR CPCU/INS. INST. OF AM., WHITE PAPER ON PREDICTIVE ANALYTICS 4–5 (2007), https://bit.ly/2ugbJRK (describing how insurers could use Big Data to improve their marketing practices).

18. *See id.*

19. *See* CORBETT ET AL., *supra* note 13, at 3–7; STACKIQ, *supra* note 13, at 3–4.

20. *See* Helveston, *Consumer Protection*, *supra* note 6, at 876; Swedloff, *supra* note 6, at 344–45.

21. *See* Swedloff, *supra* note 6, at 344–45.

they are willing to offer coverage.[22] Until the modern age, personal line insurers making underwriting decisions would collect information directly from applicants and analyze it using metrics from their claim experience databases.

The Big Data era has the potential to upset the traditional model in two ways. First, the growth of the data collection and brokering industry has provided insurers with an inexpensive mechanism for collecting large amounts of information about their applicants.[23] Given the importance of risk-assessment and underwriting in this industry, there are massive financial incentives encouraging insurers to incorporate as much data as possible into their processes. Whereas insurers in the pre-digital era would have to expend substantial resources to collect outside information about their applicants and policyholders, cost constitutes a much smaller deterrent in a tech-saturated environment.

Second, the aggregation of massive amounts of consumers' personal data and advancements in AI-driven algorithmic learning have made it possible to derive almost limitless correlations between individual characteristics and risk.[24] In the past insurers were limited to analyzing risk correlations between the relatively small set of characteristics that applicants provided in the application process and their claims experience. Cheap access to seemingly endless amounts of consumer data and improvements in AI-driven analytics have created an environment where insurers underwriting decisions could be based on AI-controlled analysis of a nearly infinite number of data points.[25]

As with the changes in advertising, it may appear as though these developments are not problematic as they simply assist insurers with performing operations that they already do. While it is true that Big Data-informed insurers will be engaging in the same type of underwriting analyses as they had in the past, the vast expansion in the amount of data they will be able to access has the potential to harm consumers in new ways. As will be explained in greater detail in the following Section, insurers expanding their data sources beyond applications and claims databases increases the risk that insurers will engage in prohibited forms of discrimination and threaten individuals' liberty interests.

22. *See* FEINMAN, *supra* note 16, at 14–15 (describing insurance companies' underwriting and rate setting operations); JEFFREY W. STEMPEL ET AL., PRINCIPLES OF INSURANCE LAW 96 (4th ed. Lexis Nexis 2012) (same).

23. *See* NYCE, *supra* note 17, at 5 (describing how predictive analytics can improve insurers' ability to detect risk factors); CORBETT ET AL., *supra* note 13, at 6 (describing how new technologies enabled an auto insurer to collect better data on its customers and identify factors that correlate with risk).

24. *See* NYCE, *supra* note 17, at 5 (describing how predictive analytics can improve insurers' ability to detect risk factors); CORBETT ET AL., *supra* note 13, at 6.

25. *See* Swedloff, *supra* note 6, at 344–45.

3. Claims Management

When policyholders file coverage claims with insurance companies, their claims are processed by the insurer's claims management division. Given the near uniformity of consumer casualty policies and the similarity of most losses, it often is not very difficult to determine whether most claims fall inside or outside the scope of coverage. Much of claims management groups' work focuses on resolving disputes with policyholders with claims where coverage is legitimately unclear and attempting to identify fraudulent claims. While it is easy to assume that insurance companies approach the handling of consumers' claims in a good faith manner, history provides a number of high-profile examples showing that at least some insurers have used this process to shirk their contractual obligations.[26]

Just as Big Data will enhance insurers' underwriting capabilities by enabling them to better assess an applicant's risk of suffering a covered loss, it will similarly enhance their claims management capabilities.[27] It is not clear whether analytics will help insurers to determine whether difficult claims fall within coverage. Insurers, however, will be able to use internal and external data sources and AI-driven analytics to better predict policyholders' reactions to the insurers' claims determinations.[28] This increase in predictive power has the potential to be used in legitimate as well as abusive manners. An example of the former would be insurers using analytics to improve their fraud detection capabilities. Examples of the latter involve insurers using analytics to increase the efficacy of their past bad faith practices—predicting which policyholders are least likely to contest a wrongful denial of coverage or estimating the amount a policyholder with a legitimate claim would be willing to accept to avoid having to take legal action.[29]

B. How Changes to Insurers' Practices Could Harm Consumers

Having identified the three areas of insurers' operations that have the greatest potential to change in a Big Data environment, it is now possible

26. *See* Kenneth S. Abraham, *Liability for Bad Faith and the Principle Without a Name (Yet)*, 19 CONN. INS. L.J. 1, 4–7 (2012–2013).

27. *See* NYCE, *supra* note 17, at 5–6 (describing how insurers could use Big Data to improve their ability to detect fraudulent claims and prioritize claims in an optimal manner).

28. *See* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1008–17 (2014).

29. *See* Abraham, *supra* note 26, at 4–7; *see also* Calo, *supra* note 28, at 1008–17, 1031–34.

to discuss how new commercial practices could injure consumers' interests. Scholars have identified a number of different ways that the introduction of social profiling into commercial markets may harm individuals.[30] While the dangers associated with the use of consumers' data in markets generally are also applicable to the insurance market, the usage of this data by insurers poses additional unique dangers.[31] This section provides an overview of both the broadly applicable and insurance-specific harms that unconstrained use of consumer data would cause.

1. Personal Liberty and Autonomy Norms

One of the general concerns that commentators have raised about life in a Big Data-driven society is that individuals' freedom of choice will be substantially diminished and there will be an increase in the degree to which their behaviors will be controlled by the state or private actors. Even though all orderly societies restrict their citizens' behaviors, protecting individuals' personal liberties and ability to make self-directed choices is generally regarded as one of the primary virtues that states should pursue. Much of existing consumer protection law, for instance, can be viewed as promoting individuals' liberty and autonomy—prohibitions on deceptive advertising protect consumers' decision-making capacity, sanctions for bad faith conduct provide a mechanism for holding individuals to their promises, etc.[32] While all transactional agreements place constraints on each of the contracting parties' autonomy, the state has attempted to protect consumers by prohibiting commercial practices that it has deemed go too far in impairing their interests.[33]

Commercial uses of analytics will impair personal liberty and autonomy in two ways. First, the mere existence of the analytics infrastructure will affect the decisions that consumers make in their private (i.e., non-commercial) lives. Businesses' interest in analytics has already created massive demand for consumer data. The collection of this data requires entities to watch and record individuals' behaviors, a role that a variety of different types of companies have stepped into.[34] These companies' acts of surveillance (as well as growing societal awareness that

30. *See, e.g.*, Citron & Pasquale, *supra* note 5, at 1; Crawford & Schultz, *supra* note 5, at 96–109; Schmitz, *supra* note 5, at 1411; Zarsky, *supra* note 5, at 1375.

31. *See* Helveston, *Consumer Protection*, *supra* note 6, at 862; Swedloff, *supra* note 6, at 344.

32. *See, e.g.*, Max Helveston & Michael Jacobs, *The Incoherent Role of Bargaining Power in Contract Law*, 49 WAKE FOREST L. REV. 1017, 1050–56 (2014) (describing commercial practices that have been prohibited through common law, legislative, and regulatory measures).

33. *Id.*

34. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 7–9 (2014) [hereinafter FTC, DATA BROKERS].

their actions are being watched) have the potential to drastically alter individuals' behaviors.

Insurance companies' ability to discriminate among consumers when selling their product substantially enhances the likelihood that their use of analytics will influence consumers' noncommercial behaviors. Unlike most businesses, the law permits insurers to exert a large degree of control over whom they sell their services to.[35] Insurers can refuse to sell policies to individuals that their underwriting procedures deem to be bad risks. Alternatively, they can increase the price of their products to account for applicants' perceived level of risk.[36] Because insurers are able to engage in these behaviors, they have the ability to create behavioral incentives that could influence potential consumers' decisions.

For example, assume that several auto insurance companies have analyzed large amounts of consumer data and found a strong correlation between purchases of highly-caffeinated drinks at gas stations and highway collisions. This information would cause these insurers to begin to incorporate this correlation into their underwriting and pricing models, causing them to either deny policies to, or charge higher premiums to, anyone that the insurer knows makes such purchases. If these insurers' practices became public knowledge, it is likely that individuals would avoid purchasing highly-caffeinated drinks at gas stations (or, at a minimum, make sure they pay for such purchases in ways that could be not traced back to them). Similar examples could be constructed that would discourage consumers from engaging in wholly non-commercial activities.

While it is possible that insurers' use of analytics could impair consumer autonomy in this way, there are reasons to believe that the impact of these practices will be relatively minimal. The primary problem with the causal mechanism outlined above is that it assumes that consumers will become aware of the behaviors that will factor into potential insurers' underwriting processes. Insurers consider their underwriting and pricing methodologies to be closely guarded secrets, so public discovery of this type of information is unlikely. Perhaps more important, however, is the fact that the underwriting decisions of Big Data-empowered insurers will be dictated by AI-derived algorithms that are

35. *Cf.* Nancy Leong & Aaron Belzer, *The New Public Accommodations: Race Discrimination in the Platform Economy*, 105 GEO. L.J. 1271, 1277–1284 (2017) (providing a background of laws prohibiting commercial entities from discriminating among consumers).

36. *Cf.* Robert M. Weiss & Ajay K. Mehrotra, *Online Dynamic Pricing: Efficiency, Equity and the Future of E-Commerce*, 6 VA. J.L. & TECH. 11, *1–4 (2001) (discussing "the historical, economic, and legal aspects" of flexible pricing).

functionally black boxes.[37] If insurers, much less consumers, are unaware of what behaviors affect their determinations, then it is hard to see how consumers' autonomy would be constrained in this way.

Second, commercial analytics will harm individuals' liberty and autonomy interests by encouraging insurers to increase the degree to which their policies control policyholders' behaviors. While most businesses have little interest in influencing individuals' conduct outside of the context of their product or service, the long-term and indemnification-centered nature of insurance agreements creates incentives for insurers to attempt to assert a greater degree of control over consumers' behaviors.[38] As insurers tap into previously inaccessible data, they will be able to identify more factors that bear on the likelihood a policyholder will suffer a loss. Once insurers have this knowledge, they will have strong financial incentives pushing them to compel policyholders to engage in risk-reducing behaviors.

Insurers regularly structure their consumer policies in ways that compel or encourage policyholders to take certain actions. For example, an insurance company could make coverage for a household contingent on the policyholder agreeing to maintain fire detection/extinguishing equipment or provide for a premium reduction if the policyholder installs security cameras.[39] The scope of the coverage offered by insurers' policies can also directly influence policyholders' behaviors. Insurers regularly issue homeowner's policies that exclude or limit the amount of coverage for losses that are due to the policyholder engaging in particular activities (e.g., having a certain breed of dog, storing certain chemicals in their house).[40]

Whether these types of insurer-imposed controls over policyholder behavior constitute objectionable infringements on consumer autonomy primarily depends on the conduct that the insurer is targeting. Traditionally, insurers have targeted behaviors that have a clear connection to the insured-against risk and that are not regarded as

37. Swedloff, *supra* note 6, at 343–44.

38. *See* Tom Baker & Rick Swedloff, *Regulation by Liability Insurance: From Auto to Lawyers Professional Liability*, 60 UCLA L. REV. 1412, 1418–30 (2014) (describing how insurers regulate policyholders' behavior to reduce risk of loss); Omri Ben-Shahar & Kyle D. Logue, *Outsourcing Regulation: How Insurance Reduces Moral Hazard*, 111 MICH. L. REV. 197, 206–12 (2012) (same).

39. *See* Baker & Swedloff, *supra* note 38, at 1418–30; Ben-Shahar & Logue, *supra* note 38, at 206–12.

40. *See* Baker & Swedloff, *supra* note 38, at 1418–30; Ben-Shahar & Logue, *supra* note 38, at 206–12; *see also* Larry Cunningham, *The Case Against Dog Breed Discrimination By Homeowners' Insurance Companies*, 11 CONN. INS. L.J. 1, 4–5, 11–17 (2004–2005).

infringing upon individuals' zone of personal liberty.[41] For instance, insurers providing small business owners with property and general liability coverages might require the owner to install sprinkler systems and retain security personnel.[42] Both of these requirements have apparent relationships with the risks being insured against and neither compel the policyholder to take actions that most would regard as falling within the personal sphere.

While policyholders have found the majority of the actions required by insurers to be unobjectionable, this has not uniformly been the case. When insurance companies have adopted behavior-forcing practices that do not clearly satisfy both of these criteria, consumers have argued that they were being unfairly coercive. When a disability insurer began refusing to issue policies to individuals who disclosed that they were taking an HIV-prevention medicine there was prompt public backlash against the company.[43] Denying insurance coverage to individuals due to their decision to take a prophylactic medicine clearly intrudes on individuals' zone of liberty, as well as being questionable under the direct-relationship test. Similarly, there has been robust criticism of companies that have refused to issue homeowners' coverage to individuals with pets of certain species or breeds.[44] Not only is it unclear whether there is actually a direct connection between owning these particular types of pets and increased risk of loss, but these practices impair individuals' ability to engage in personal conduct that the law permits.[45]

As insurers incorporate Big Data analytics into their operations, the concern is that they will increase the degree to which they seek to regulate policyholder behaviors and will do so in ways that constrain individuals' personal freedoms.[46] The digital revolution and the growing accessibility

41. What interests constitute protected liberty interests has never been exhaustively determined, but several specific examples have been identified in case law. *See, e.g.*, Meyer v. Nebraska, 262 U.S. 390, 399 (1923).

42. These types of promises typically appear in the endorsements that insurers attach to the policies they issue to customers. Endorsements add additional terms to the policy, expanding or limiting the coverage set forth in the policy. *See*, *e.g.*, Am. Way Cellular v. Travelers Prop. Cas. Co. of Am., 157 Cal. Rptr. 3d 385, 389 (Cal. Ct. App. 2013); Indus. Dev. Ass'n v. Commercial Union Surplus Lines Ins. Co., 536 A.2d 787, 789–90 (N.J. Super. Ct. App. Div. 1988); Holz Rubber Co. v. Am. Star Ins. Co., 533 P.2d 1055, 1059–61 (Cal. 1975) (en banc); Port Blakely Mill Co. v. Springfield Fire & Marine Ins. Co., 106 P. 194, 194–96 (Wash. 1910).

43. Donald G. McNeil Jr., *He Took a Drug to Prevent AIDS. Then He Couldn't Get Diability Insurance*, N.Y. TIMES (Feb. 12, 2018), https://www.nytimes.com/2018/02/12/health/truvada-hiv-insurance.html.

44. *See* Cunningham, *supra* note 40, at 4–5, 11–17.

45. *Id.*

46. *See* Jay Stanley, *The Potential Chilling Effects of Big Data*, ACLU BLOG (Apr. 30, 2012), https://www.aclu.org/blog/technology-and-liberty/potential-chilling-effects-big-data; *see also* Bill Davidow, *Redlining for the 21st Century*, ATLANTIC (Mar. 5, 2014),

of data will allow insurers to discover increasingly indirect correlations between individual characteristics and risk. Competitive pressures will push insurers to incorporate these correlations into their underwriting and contract design practices. While some of these behavior-modifying changes will be unobjectionable, it is likely that others will intrude on the personal spheres of consumers. An example of this already beginning to occur can be found in reports that some insurers have debated whether they should require individuals seeking homeowner's coverage to install monitoring equipment in their homes.[47]

2. Anti-discrimination Norms

Another concern that has been raised about the integration of Big Data analytics into consumer markets is that it will result in increased discrimination against certain classes of individuals. The multitude of anti-discrimination[48] and public accommodation laws[49] currently in force establish that modern society embraces anti-discrimination norms in the commercial sphere. While there is variance in which personal qualities are protected in different contexts, it is clear that attempts by commercial actors to treat consumers differently on the basis of immutable or deeply personal (e.g., religious affiliation, marital status) characteristics are generally viewed unfavorably.

There are reasons to believe that these anti-discrimination norms are particularly strong in the domain of insurance. Insurance companies are no different than other commercial entities in that they have had to comply with state and federal laws that generally proscribe discriminating among consumers in particular ways. Regulators in many states have supplemented these laws by imposing additional anti-discrimination rules in the insurance context.[50] Even though some consider the laws governing

http://www.theatlantic.com/business/archive/2014/03/redlining-for-the-21st-century/284235 (describing prohibitions against redlining and how Big Data could lead to unfair discrimination in the commercial sector).

47. *See* ERNST & YOUNG, 2013 U.S. PROPERTY/CASUALTY INSURANCE OUTLOOK 5 (2012) ("While the automobile lines of business are the initial beneficiaries of Big Data, opportunities are emerging in homeowners insurance (among others), with video monitors, security systems and gaming systems all collecting and transmitting usable data.").

48. *See, e.g.,* Age Discrimination in Employment Act of 1967, 29 U.S.C. ch. 14 (2012 & Supp. 2017); Title VII of the Civil Rights Act of 1964, 42 U.S.C. ch. 21, subch. VI (2012 & Supp. 2017); Americans With Disabilities Act of 1990, 42 U.S.C. ch. 126 (2012 & Supp. 2017).

49. Joshua Block, *Businesses Do Not Have a License to Discriminate*, ACLU BLOG (Dec. 18, 2012), https://www.aclu.org/blog/lgbt-rights-free-speech-religion-belief/businesses-do-not-have-license-discriminate (describing state public accommodation laws).

50. *See* Ronen Avraham et al., *Understanding Insurance Antidiscrimination Laws*, 87 S. CAL. L. REV. 195, 232–62 (2014) (collecting state anti-discrimination laws).

insurers' conduct to be insufficiently robust,[51] it is clear that existing legal structures impose limits on insurers' ability to treat consumers differently.

Scholars have raised doubts about the degree to which insurance companies comply with existing anti-discrimination laws.[52] Few, if any, of these claims allege that insurers are intentionally discriminating against members of protected classes because of their membership in that class. The most common concern that has been raised is that insurers are indirectly discriminating against protected classes when they base their decisions on criteria that are highly correlated with protected class membership.[53]

If insurers incorporate Big Data analytics into their operations in the manners described earlier, it will become more likely that they will treat individuals differently in ways that appear to be based on protected characteristics. The basic premise underlying AI-driven analytics is that computers are able to analyze incredible amounts of data and identify relationships that would have been difficult to impossible to detect through other means. In the context of underwriting, this would involve using artificial intelligence to find relationships between policyholder-related (or location-related) data and the likelihood that a loss covered by the insurance policy will occur. The specific algorithm derived from this analysis would be dynamic, with the formula being constantly updated to account for new data.[54] It is important to note that the algorithms created

51. *See id.* at 197–99, 267 ("Our findings reveal various discrepancies between the reality of state insurance antidiscrimination law and the largely theoretical literature on the topic. . . . [S]uch laws often have little to say about the most important and divisive types of discrimination: distinctions based on race, national origin, or religion.").

52. *See, e.g.*, Regina Austin, *The Insurance Classification Controversy*, 131 U. PA. L. REV. 517, 517 (1983) (discussing general tactics insurers can use to discriminate without violating anti-discrimination laws); Mary L. Heen, *Nondiscrimination in Insurance: The Next Chapter*, 49 GA. L. REV. 1, 3–7 (2014); Alan I. Widiss, *To Insure or Not To Insure Persons Infected with the Virus that Causes AIDS*, 77 IOWA L. REV. 1617, 1658–64 (1992) (describing how insurers could legally discriminate against sexual and racial minorities via HIV testing); Robert Pear, *Health Insurers Skirt New Law*, *Officials Report*, N.Y. TIMES, (Oct. 5, 1997), https://www.nytimes.com/1997/10/05/us/health-insurers-skirting-new-law-officials-report.html (describing how health insurers were able to skirt laws intended to protect sick individuals); *see also* Jessica Mason Pieklo, *Four Insurance Companies Accused of Widespread Sex Discrimination,* REWIRE.NEWS (Jan. 17, 2014), https://rewire.news/article/2014/01/17/four-insurance-companies-accused-widespread-sex-discrimination/.

53. *See, e.g.*, Katy Chi-Wen Li, *The Private Insurance Industry's Tactics Against Suspected Homosexuals: Redlining Based on Occupation, Residence and Marital Status*, 22 AM. J.L. & MED. 477, 479–80 (1996); Willy E. Rice, *Race, Gender, "Redlining," and the Discriminatory Access to Loans, Credit, and Insurance*, 33 SAN DIEGO L. REV. 583, 609–16 (1996).

54. *See* Thomas H. Davenport, *Industrial-Strength Analytics with Machine Learning*, WALL ST. J. (Sept. 11, 2013), http:// http://blogs.wsj.com/cio/2013/09/11/industrial-strength-analytics-with-machine-learning/.

by AI-driven analytics are essentially black boxes—there is no way to know what characteristics the formula is taking into consideration when making a prediction.[55]

In the pre-analytics environment, an insurer that wished to comply with anti-discrimination laws could simply review the criteria they used to make a decision and make sure that none of its factors targeted (or served as a proxy for) a protected class. It is unclear how insurers relying on AI-derived algorithms will be able to do the same.[56] Further, given the nature of machine learning, it seems probable that at least some of the characteristics that the algorithm operates on will be strongly correlated with an individual's membership in a protected class.[57]

In summary, analytics-driven insurers will be more likely to violate broadly held anti-discrimination norms. If AI-derived algorithms begin to play a primary role in insurers' operations, then it is likely that these companies' advertising, underwriting, and claims handling practices will treat individuals differently in ways that correlate strongly to protected characteristics.

3. Egalitarianism Norms

While equality-centered norms do not play a substantial role in most commercial markets, they can be found in insurance markets. This can be attributed to the fact that insurers, unlike most vendors, are permitted to discriminate against consumers in ways that are not permitted in other contexts. Throughout the academic literature on the function and regulation of insurance markets one can find discussions about when and how insurers should be allowed to deny individuals access to insurance or charge different rates to those possessing certain characteristics.[58] Similar debates exist about whether the ideal insurance system would be one that charges all policyholders actuarially accurate rates or one that spreads risk in a way that mitigates differences in individuals' risk profiles that are

55. Swedloff, *supra* note 6, at 363 ("The far more likely scenario is that it will not be readily apparent to anyone why some individuals are charged more. The algorithms driving big data will simply spit out higher prices for some policyholders than others.").

56. Swedloff, *supra* note 6, at 370–71 (describing the types of analyses regulatory bodies would have to do to detect this form of discrimination); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671, 712 ("Data mining allows employers who wish to discriminate on the basis of a protected class to disclaim any knowledge of the protected class in the first instance . . . .").

57. Swedloff, *supra* note 6, at 370.

58. *See* Avraham et al., *supra* note 50, at 232–62 (discussing limitations on insurers' ability to discriminate against consumers).

attributable to luck (or other factors that an individual did not choose).[59] Regardless of which view one subscribes to, it is clear that changes in the insurance industry that caused it to be less egalitarian would cause a substantial harm to many consumers.

The use of Big Data analytics in insurers' operations could result in a system that exacerbates individuals' luck-based characteristics. As insurance companies' algorithms include larger and larger numbers of correlations between risk and individual qualities, it will become more likely that an insurers' interactions with a consumer will be driven by factors that the consumer had little to no control over. Many of the qualities that AI-driven analytics might identify as increasing the likelihood that a policyholder will experience a loss (or submit a fraudulent claim) are things that are immutable, luck-based, or otherwise non-elected.[60] Using these characteristics as criteria for determining which individuals receive preferential treatment would lead insurers to violate fairness norms by treating some consumers better than others on the basis of fortuity alone.[61]

While insurers treating individuals differently on these grounds would in and of itself be contrary to equality norms, the potential harm associated with these practices is much greater. This is because many of the non-elected characteristics that would flag an individual as being a greater risk to an insurer are also qualities that put individuals at a disadvantage in society generally.[62] It is likely that the converse is true as well—qualities indicating individuals present a low risk also provide individuals with societal advantages.[63] As a hypothetical example, if individuals that are born into high-poverty areas are more likely to be involved in a car accident due to another driver's negligence and an auto insurers' algorithm charges higher rates to individuals who have been in prior accidents regardless of their fault, then that insurer's practices will exacerbate, rather than mitigate, the impact that consumers' unelected characteristics will have on their lives.[64]

59. *See* JOHN RAWLS, A THEORY OF JUSTICE 11–17 (1974) (describing modern conception about the relationship of justice, desert, and morality); Heen, *supra* note 52, at 10–23.

60. Helveston, *Consumer Protection*, *supra* note 6, at 896.

61. *Id.* at 895–97.

62. *See* EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 46–47 (May 2014), https://bit.ly/2HQiQrw (expressing concern that businesses using analytics to discriminate among customers will hurt the least well off).

63. *Id.*

64. *See* Swedloff, *supra* note 6, at 348–51. Insurers' practices already take some of these types of characteristics into account when making pricing and underwriting decisions, but the data revolution could drastically expand the number of such qualities that factor into an individual's ability to procure insurance.

4. Good Faith Norms

A final market norm that could be injured by insurers' use of Big Data analytics is the basic presumption that commercial entities will deal with consumers fairly and honor their contractual obligations. The idea that both parties in a contractual relationship have an obligation to fully perform their end of the bargain is one of the fundamental ideas in modern society.[65] This is particularly true in the context of consumer contracts, where the law has attempted to protect individuals from being exploited by more sophisticated commercial entities.[66] One example of how the legal system has done this is by policing businesses' attempts to take actions that, while technically within the bounds of their agreement, constitute unfair abuses of discretion.[67]

The terms of insurance contracts make insurers' obligations to cover policyholder losses dependent on several conditions being met, while also vesting insurers with the authority to determine whether those conditions have been satisfied. This structure ends up providing insurers with a large degree of discretion over when their performance obligations are triggered. Once a policyholder has filed a claim, an insurer can determine that the claim is fully covered, that only certain aspects of the claim will be covered, that the claim falls outside of coverage, that the loss was covered but the policyholder's failure to perform their contractual duties vitiated coverage, etc. One of the longstanding issues in insurance regulation has been how the state should make sure that insurers are not using unfair claims handling practices to shortchange policyholders.[68] More specifically, scholars and regulators have raised concerns that absent regulatory measures, insurers will abuse consumers' lack of knowledge and the high transaction costs that consumers must incur to contest

65. *See* Emily M.S. Houh, *Critical Interventions: Toward an Expansive Equality Approach to the Doctrine of Good Faith in Contract Law*, 88 CORNELL L. REV. 1025, 1033 (2003) ("The implied obligation of good faith and fair dealing has been adopted by the *Restatement (Second) of Contracts*, is implied into every contract governed by the Uniform Commercial Code, and in most jurisdictions is implied into every contract at common law."); James A. Webster, Comment, *A Pound of Flesh: The Oregon Supreme Court Virtually Eliminates the Duty to Perform and Enforce Contracts in Good Faith*, 75 OR. L. REV. 493, 497–509 (1996) (discussing the history of the good faith contractual obligation).

66. *See* Helveston & Jacobs, *supra* note 32, at 1017.

67. *See* Emily M.S. Houh, *The Doctrine of Good Faith in Contract Law: A (Nearly) Empty Vessel?*, 2005 UTAH L. REV. 1, 5–12 (2005).

68. *See, e.g.*, Whitney R. Mauldin, *Good Business/Bad Faith: Why the Insurance Industry Should Adopt a Good Faith Model*, 44 TORT TRIAL & INS. PRAC. L.J. 151, 159 (2008). *See generally* Hugh A. Linstrom, *Unfair Claims Settlement Practices: A Summary of California Law*, 15 WHITTIER L. REV. 691 (1994); FEINMAN, *supra* note 16.

insurers' determinations to get away with awarding policyholders less than they are entitled to, or denying legitimate claims entirely.[69]

Once insurers begin utilizing Big Data analytics to improve their claims management systems, there is a substantial risk that they will act in ways that violate good faith norms. Consumer analytics will not only enable insurers to get a better idea of which individuals pose larger risks than others, but will also allow them to identify individuals that are more or less likely to contest an insurers' finding that their claim is not covered.[70] Insurers with this type of knowledge will be able to adopt abusive claims management practices, wherein they intentionally deny the valid coverage claims (or offer policyholders less than they are entitled to) of individual they know are unlikely to bring suit against the insurer. While the good-natured might believe that insurers would never engage in this type of conduct, there have been several examples of companies doing essentially the same acts.[71]

III. PART II - STATUTORY RESTRICTIONS ON THE USE OF CONSUMER DATA

This Part provide a description of three of the most important laws that limit commercial entities' possession and use of consumer data. Each law was enacted by different legislative bodies—the California Consumer Privacy Act was passed by the California state legislature, the Vermont Data Broker Act was passed by the Vermont legislature, and the Fair Credit Reporting Act was enacted by the federal legislature—and each targets significantly different conduct. After providing an overview of each law and analyzing how it constrains insurance companies' conduct, Part III will assess whether these laws are sufficient to address the concerns identified in Part I and discuss how regulatory shortfalls should be addressed.

A. The Fair Credit Reporting Act

The Fair Credit Reporting Act[72] ("FCRA") was enacted by Congress in 1970. The statute's statement of purpose provides that the FCRA was meant to ensure that inaccurate credit reports would not "directly impair the efficiency of the banking system, and unfair credit reporting methods [would not] undermine the public confidence which is essential to the

69. *See supra* note 68.
70. *See* Calo, *supra* note 28, at 1008–17, 1031–34.
71. *See* Abraham, *supra* note 26, at 7.
72. Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1127 (1970) (codified as amended at 15 U.S.C. §§ 1681–1681x).

continued functioning of the banking system."[73] In order to achieve this goal, the FCRA establishes a set of rules meant to "insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy."[74]

The FCRA operates by categorizing entities that collect certain types of consumer information as "credit reporting agencies" ("CRAs") and then placing restrictions on the conduct of CRAs as well as any companies that use information that is provided by a CRA. It also imposes requirements on entities that provide information to CRAs.[75] The FCRA defines a "credit reporting agency" as an entity that regularly "assembl[es] or evaluat[es] consumer credit information or other information on consumers for the purposes of furnishing consumer reports to third parties" and uses any means of interstate commerce when doing so.[76] The act's definition of "consumer reports" provides context on the types of information that the act is concerned with regulating. A "consumer report" is first defined as any communication "by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living."[77] Communications of these types only qualify as consumer reports, however, if they are "used or expected to be used . . . as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under [another section of the act]."[78]

The FCRA limits consumer reporting agencies' ability to sell consumer data. It prohibits agencies from providing third parties with consumer reports unless the disclosure falls under one of the statute's authorized purposes.[79] Most relevant for purposes of this discussion are the provisions allowing consumer reports to be provided "[t]o a person which [the consumer reporting agency] has reason to believe . . . (C) intends to use the information in connection with the underwriting of insurance involving the consumer; or . . . (F) otherwise has a legitimate business need for the information (i) in connection with a business transaction that is initiated by the consumer; or (ii) to review an account to determine whether the consumer continues to meet the terms of the

73. *Id.* § 602(a)(1), 84 Stat. at 1128.
74. *Id.* § 602(a)(4), 84 Stat. at 1128.
75. *See* 15 U.S.C. § 1681s-2 (2012 & Supp. 2017).
76. 15 U.S.C. § 1681a(f) (2012 & Supp. 2017).
77. *Id.* § 1681a(d)(1).
78. *Id.*
79. *See* 15 U.S.C. § 1681b (2012 & Supp. 2017).

account."[80] The act further specifies that a consumer report can only be furnished in connection with an insurance transaction that is not initiated by the consumer if the consumer provides their consent or "the transaction consists of a firm offer of . . . insurance."[81]

The part of the FCRA that is most relevant to the concerns raised in Part I are the requirements the statute imposes on entities that use consumer report information. If an individual takes an "adverse action" against a consumer on the basis of information contained in a consumer report the act requires the individual to provide that consumer with a notice.[82] The notice must inform the consumer of the adverse action taken, the contact information for the CRA that furnished the consumer report, a statement that the CRA did not take the adverse action, and a summary of the consumer's right to obtain a copy of their consumer report from the CRA as well as their right to dispute the accuracy or completeness of any information in the CRA's consumer report.[83] While the act also contains requirements for entities that take adverse actions against consumers based on information obtained from non-CRAs, these provisions only apply to entities making credit (not insurance) related decisions.[84] Finally, the FCRA requires that insurers that make offers of insurance to individuals on the basis of information contained in a consumer report include certain disclosures in their offers and mandates that they maintain files describing the basis on which offers were made.[85]

The extent to which the FCRA limits insurance companies' ability to incorporate Big Data analytics into their operations depends on the resolution of a few key issues. First, what constraints does the FCRA put on insurers' use of information purchased from the types of data brokers discussed in Part I? Second, when an insurer uses information from a consumer report, what types of behaviors would constitute an "adverse action" against a consumer? Third, what penalties would insurers face if they violate the FCRA?

Whether the FCRA will affect the use of Big Data analytics in the consumer insurance industry largely depends on whether the data insurers purchase from brokers are considered consumer reports. If the data counts as a consumer report, then insurers will be subject to the FCRA's

80. *Id.* § 1681b(a)(3).

81. *Id.* § 1681b(c)(1)(B)(i). If a consumer report is being disclosed in connection with a firm offer of insurance, then there are additional requirements that must be met (e.g., that the consumer reporting agency has complied with the FRCA's opt-out requirements). *See id.* § 1681b(c)(2).

82. *See* 15 U.S.C. § 1681m (2012 & Supp. 2017).

83. *See id.* § 1681m(a).

84. *See id.* § 1681m(b)(1).

85. *See id.* § 1681m(d).

restrictions on the procurement and use of this information. If the data does not count as a consumer report, then the FCRA poses no barrier.

As a matter of first impression, it would appear as though insurers purchasing consumer data from brokers would constitute a sale of a consumer report. Such data would certain be a "communication . . . bearing on a consumer's credit worthiness, credit capacity, character, general reputation, personal characteristics, or mode of living" and the data would be "used or expected to be used . . . as a factor in establishing the consumer's eligibility for . . . credit or insurance . . . [or] employment."[86]

There are two problems with this analysis. First, in order for a transmission of data to qualify as a consumer report, it must be sold by an entity that is a consumer reporting agency.[87] The definitions of consumer report and consumer reporting agency are interdependent, as the primary defining characteristic of an agency is that it "regularly engages in . . . the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties."[88] Digital data brokers do not appear to categorically qualify as consumer reporting agencies. The FTC has only filed FCRA enforcement actions against a limited number of data brokers.[89] In its complaints, the agency has argued that these data brokers were CRAs because they marketed their products in ways that meant the brokers knew their information would be used in making employment decisions.[90] The fact that the FTC has only pursued actions against certain data brokers indicates that the agency believes that the remainder do not engage in activities that would cause them to be CRAs and, hence, any data they sell cannot be considered a consumer report.

Second, for at least some of the ways that insurers might seek to use this data, it does not appear as though insurers would be using this data as "a factor in establishing the consumer's eligibility" for insurance. For instance, an insurer could purchase large amounts of consumer data from data brokers and exclusively use that data to create algorithms and profile individuals for marketing or claims management purposes. Further, because the definition of consumer report requires there to be a direct connection between the data communicated and a determination of a specific individual's eligibility for insurance, it is possible that insurers

86. 15 U.S.C. § 1681a(d) (2012 & Supp. 2017).

87. *See* FED. TRADE COMM'N, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT 1 (July 2011), https://bit.ly/2n9mkXt [hereinafter FTC, FAIR CREDIT REPORTING ACT].

88. 15 U.S.C. § 1681a(f).

89. *See* FTC, BIG DATA, *supra* note 13, at 14.

90. *Id.*

could use this data to create their general underwriting algorithms. This interpretation is supported by a Federal Trade Commission report stating that "[i]nformation that does not identify a specific consumer does not constitute a consumer report even if the communication is used in part to determine eligibility."[91]

The foregoing establishes that insurers will not be limited by the FCRA when purchasing information from data brokers and engaging in certain types of analytics. The FCRA will, however, apply to at least one type of conduct—insurers purchasing an individual's information for use when making underwriting determinations for that specific individual. Indeed, there have been several lawsuits against insurers alleging that they failed to satisfy the FCRA's requirements for entities that use consumer report information when underwriting.

Many of the FCRA-based claims brought against insurers have alleged that the insurers failed to provide consumers with a required adverse action notice. While the statute contains a relatively clear definition of "adverse action,"[92] in the insurance context, whether specific insurer actions constitute adverse actions has been a hotly contested matter. The Supreme Court of the United States addressed this issue in *Safeco Insurance Co. v. Burr*.[93] In *Safeco*, the central dispute was whether an insurer was required to provide an adverse action notice when it issued an initial coverage offer to a consumer with a rate that was negatively affected by information in a consumer report.[94] The Court held that insurers must give adverse action notices even on initial policies if the rate the insurer charges is more than what the insurer would have charged in the absence of any of the information in the consumer report.[95] Thus, it is clear that the FCRA does impose some requirements on insurers in the underwriting context.

An insurer that violates the FCRA can find itself the subject of both administrative and civil enforcement actions. For administrative actions, the Federal Trade Commission has primary enforcement authority and is explicitly authorized to file civil suits against individuals that knowingly violate the act.[96] Courts can assess penalties of up to $2,500 per violation, taking into account factors such as the violator's degree of culpability,

91. FTC, FAIR CREDIT REPORTING ACT, *supra* note 87, at 20. Given this interpretation, it appears that whether the FCRA permits insurers to do this depends on if the insurer could reasonably link the data supplied by the broker back to specific consumers.

92. 15 U.S.C. § 1681a(k)(1)(B)(i).

93. Safeco Ins. Co. v. Burr, 551 U.S. 47 (2007).

94. *See id.* at 59–61.

95. *See id.* at 61–62.

96. 15 U.S.C. § 1681s(a) (2012 & Supp. 2017).

history of similar conduct, and ability to pay.[97] Other federal and state actors have limited authority to pursue violations of the act.[98]

The FCRA has two civil enforcement provisions that consumers could use to bring actions against insurers. First, individuals are authorized to bring civil suits alleging that an insurer negligently failed to comply with the act's requirements.[99] If successful, they would be able to recover "any actual damages sustained . . . as a result of the failure . . . [and] the costs of the action together with reasonable attorney's fees as determined by the court."[100] Second, individuals can bring claims alleging that an insurer willfully failed to comply with the act's requirements.[101] In order for a violation to be willful, it must be shown that the insurer's reading of the statute was objectively unreasonable.[102] If successful, a claimant would be able to recover "any actual damages sustained . . . as a result of the failure . . . of not less than $100 and not more than $1,000," attorney's fees, costs, and "such amount of punitive damages as the court may allow."[103] It should be noted that the FCRA explicitly exempts individuals from being held liable for violating the requirements placed on users of consumer reports if they can show "by a preponderance of the evidence that at the time of the alleged violation he maintained reasonable procedures to assure compliance."[104]

B. The California Consumer Privacy Act

The California Consumer Privacy Act of 2018 ("CCPA") was signed into law by California Governor Jerry Brown on June 28th, 2018.[105] The legislation's stated goal is "to further Californians' right to privacy by giving consumers an effective way to control their personal information"[106] and has been hailed as the most expansive privacy legislation in US history.[107] In recognition of the expansive requirements that the act places on commercial entities, the law has provided individuals

97. *Id.* § 1681s(a)(2)(A)–(B).
98. *Id.* § 1681s(b)–(c).
99. 15 U.S.C. § 1681o(a) (2012 & Supp. 2017).
100. *Id.* § 1681o(a)(1)–(2).
101. 15 U.S.C. § 1681n (2012 & Supp. 2017). The FCRA also contains a provision that authorizes consumer reporting agencies to sue any person "who obtains a consumer report from a consumer reporting agency under false pretenses or knowingly without a permissible purpose." 15 U.S.C. § 1681n(b).
102. *See* Safeco v. Burr, 511 U.S. 47, 69 (2007).
103. § 1681n(a).
104. 15 U.S.C. § 1681m(c).
105. Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES, (June 28, 2018), https://nyti.ms/2tGjAaf.
106. Assemb. B. 375, 2017–2018 Leg. § 2(i), Reg. Sess. (Cal. 2017).
107. Purvi Patel et al., *The 2018 California Consumer Privacy Act*, MORRISON FOERSTER (Jun 29, 2018), https://bit.ly/2DEzGWQ.

with a substantial period of time to bring their operations in compliance with its rules.[108]

The CCPA seeks to protect individuals' privacy rights by providing California citizens with a number of distinct rights. It grants consumers the right to know what personal information is being collected about them, as well as the right to know whether their personal information is sold or disclosed and to whom. Further, it requires that companies allow consumers to access personal information the business possesses about them. Finally, it empowers individuals to prevent companies from selling their personal information and guarantees that those that exercise their privacy rights will be given equal services and prices as those who do not.[109]

The act's two primary mechanisms for giving individuals these rights are the imposition of disclosure and access requirements on business entities that collect consumer data and the recognition that individuals have pseudo-property rights in their personal data. The CCPA's disclosure and access requirements are similar in kind to those of the FCRA. Any business that collects a consumer's personal information must, before or at the time of collection, disclose the types of data it is collecting and how it will use the information.[110] Additionally, companies must provide a consumer with a mechanism for making a "verifiable consumer request"[111] and, upon receiving such a request, must provide information about the data it possesses on the consumer.[112]

The act grants consumers rights that allow them to control how others may and may not use their personal information. First, the CCPA authorizes individuals to demand that companies delete any personal information about themselves that they possess.[113] There are important exceptions to the right to deletion—for example, companies are not required to delete consumer data if it is needed for statutorily-specified purposes,[114] which include businesses using the data internally for purposes that are consistent "with the context in which the consumer provided the information" or "reasonably aligned with" consumer expectations.[115] Second, the CCPA requires businesses that sell consumers' personal information to provide a conspicuous means for individuals to opt-out of the sale of their information and to immediately

108. CAL. CIV. CODE § 1798.198 (West 2019).
109. Assemb. B 375, § 2(i).
110. CAL. CIV. CODE § 1798.100(b) (West 2019).
111. CAL. CIV. CODE § 1798.130 (West 2019).
112. CAL. CIV. CODE § 1798.100(c).
113. CAL. CIV. CODE § 1798.105(a)–(c) (West 2019).
114. *Id.* § 1798.105(d).
115. *Id.* § 1798.105(d)(7), (9).

comply with any requests they receive.[116] Third, the act forbids companies that purchase a consumer's data from selling that data to other parties unless the consumer is provided notice of the proposed sale and consents to the transaction.[117] Finally, the CCPA prohibits companies from discriminating against consumers that exercise the rights created by the act.[118] It explicitly identifies price discrimination and refusals to deal as practices that are not permitted.[119] Perhaps paradoxically, however, the act appears to allow businesses to offer individuals financial incentives to consent to the collection and sale of their data.[120] These rights constitute a substantial departure from how the law has traditionally treated personal data, as they grant consumers' a property-like interest in their personal information.

The CCPA defines "personal information" in an expansive manner. Any information that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household[]" qualifies as personal information.[121] A non-exhaustive list of examples includes "[i]dentifiers such as real name, alias, . . . unique personal identifier, [and] online identifier[] Internet Protocol address,"[122] "Internet or other electronic network activity information, including . . . browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement[,]"[123] and "[i]nferences drawn from any of the other information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behaviors, attitudes, intelligence, abilities, and aptitudes."[124] The act explicitly notes that information that is publicly available from government records does not count as personal information.[125]

While the CCPA is a California state law, the act's requirements will end up applying to a substantial number of out-of-state and international businesses.[126] The key issue when determining whether an entity falls

116. CAL. CIV. CODE § 1798.120(a) (West 2019).
117. CAL. CIV. CODE § 1798.115(d) (West 2019).
118. CAL. CIV. CODE § 1798.125 (West 2019).
119. *Id.* § 1798.125(a)(1)(A)–(B).
120. *Id.* § 1798.125(b)(1).
121. CAL. CIV. CODE § 1798.140(*o*) (West 2019).
122. *Id.* § 1798.140(*o*)(1)(A).
123. *Id.* § 1798.140(*o*)(1)(F).
124. *Id.* § 1798.140(*o*)(1)(K).
125. *Id.* § 1798.140(*o*)(2).
126. Sam Pfeifle & Rita Heimes, *New California Privacy Law to Affect More Than Half A Million US Companies*, INT'L ASS'N OF PRIVACY PROF'LS: THE PRIVACY ADVISOR (July 2, 2018), http://bit.ly/2WljvIy.

within the scope of the CCPA is whether it qualifies as a "business." Under the act a company constitutes a "business" if it satisfies two elements:

> (1) it is a for-profit business "that collects consumers' personal information, or on the behalf of which such information is collected and that . . . determines the purposes and means of the processing of consumers' personal information, that does business in the State of California," and
>
> (2) (a) has gross annual revenues in excess of $25,000,000; (b) annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices; or (c) derives 50 percent or more of its annual revenues from selling consumers' personal information.[127]

This definition means that essentially all data brokers and every large insurer that does business in California will fall within the scope of the CCPA.

Finally, the CCPA is designed to be primarily enforced by the California attorney general. The law grants enforcement powers to the state attorney general and authorizes civil penalties ranging from $2,500 to $7,500 per violation of the act.[128] The CCPA also authorizes consumers to bring actions against businesses that fail to comply with specific statutory requirements. This private right of action, however, is rather limited, as individuals can only bring data breach claims.[129] These include allegations that a company failed to implement "reasonable security procedures and practices" and that this failure led to "unauthorized access and exfiltration, theft, or disclosure" of their personal information.[130] Courts are limited to awarding damages of actual damages or no less than $100 and no more than $750 per violation.[131]

Whether the CCPA will effectively prevent abusive uses of Big Data analytics in the consumer insurance industry depends on a variety of factors. First, there is the issue concerning which businesses will fall within its scope. Based on the statute's definition of business, it is clear that any company that primarily engages in the collection and sale of consumer data (i.e., data brokers) and does business in California will be required to comply with its rules. Most insurers selling consumer lines in California are also likely to qualify as CCPA businesses. The majority of consumer policies sold in the state are issued by for-profit businesses and

127. CAL. CIV. CODE § 1798.140(c).
128. CAL. CIV. CODE § 1798.155 (West 2019).
129. CAL. CIV. CODE § 1798.150(a)(1) (West 2019).
130. *Id*.
131. *Id*.

as part of their standard operations insurers collect and use consumers' personal information. While some insurers may be exempt because they have gross annual revenues that are less than $25,000,000 and do not receive the personal information of 50,000 or more consumers, many of the larger companies will qualify under one (or both) of these criteria.

The prevalence of individuals exercising the rights granted by the CCPA is a second issue that will be important. For example, if very few people opt-out from data brokers being able to sell their information to third-parties, then the CCPA will not pose a barrier to insurers' acquisition of consumer data. Conversely, if large numbers of individual opt-out, then insurers' only means for getting this information would be to collect it themselves.

The frequency with which individuals invoke the right to deletion and how the statutory exceptions to this right are interpreted will also play a large role in determining the law's effectiveness. While the CCPA grants consumers the ability to have businesses delete any of the consumer's personal information they possess, the optional nature of this right means that its impact will depend substantially on how often it is exercised. Further, the CCPA allows companies to keep consumer data even if a deletion request is made if "it is necessary for the business or service provider to maintain the consumer's personal information in order to . . . protect against malicious, deceptive, fraudulent, or illegal activity . . . [or t]o enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business."[132] The exact meaning of these statutory exceptions is unclear and they could be interpreted in ways that would allow insurance companies to hold on to any consumer data it possesses that it can link to its underwriting, pricing, or fraud detection operations.

A final issue that will directly impact the degree to which the CCPA impairs insurers' use of Big Data analytics is the amount of resources the state will dedicate to enforcing the law. While a bill has been introduced to expand consumers' ability to sue businesses under the statute, at present enforcement authority for the act is dependent on actions brought by state officials. If the state does not invest considerable resources into punishing non-compliant companies, then it will become increasingly likely that the CCPA will not change private actors' behaviors.

132. CAL. CIV. CODE § 1798.105(d) (West 2019).

C. The Vermont Data Broker Law

In May of 2018, the Vermont legislature became the first in the nation to pass a consumer protection law that specifically targets data brokers.[133] The stated goals of the legislation are: to provide consumers with necessary information about the operations of these companies and their right to opt-out; to ensure that consumers' data is protected by adequate security; and to create a cause of action that consumers can use to protect themselves from wrongful uses of their data.[134] The act also requires all data brokers that do business in Vermont to register with the Secretary of State, pay fees, and make annual disclosures about their operations.[135] It also imposes data security requirements on brokers.[136] The act does not, however, require data brokers to allow consumers to opt-out of having their data collected or sold.[137]

Under the act, a company counts as a data broker if it "knowingly collects and sells or licenses to third parties the . . . personal information of a consumer with whom the business does not have a direct relationship."[138] Examples of what constitutes a direct relationship include a consumer being a past or present customer, client, subscriber, employee, or investor of the business.[139]

The act's definition of what constitutes personal information is substantially less robust than the CCPA—it lists pieces of information that directly bear on an individual's identity (e.g., name, address, Social Security number) and does not explicitly include information like an individual's web-browsing history or personal preferences.[140] While the definition does include a provision that could be viewed as a catch-all—"other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty"—it seems as though personal information under the Vermont law will have a relatively narrow scope.[141] Guidance issued by the state's Attorney General, however, indicates that the catch-all provision was intended to include any set of information that could

133. An Act Relating to Data Brokers and Consumer Protection, No. 171, 2018 Vt. Acts & Resolves 584; *Vermont Enacts Nation's First Data Broker Legislation*, HUNTON ANDREWS KURTH: PRIVACY & INFO. SEC. LAW BLOG (June 13, 2018), http://bit.ly/2JXkA2G.

134. § 1, 2018 Vt. Acts & Resolves at 584–86.

135. VT. STAT. ANN. tit. 9, § 2446 (2018).

136. VT. STAT. ANN. tit. 9, § 2447 (2018).

137. VT. OFFICE OF ATT'Y GEN., GUIDANCE ON VERMONT'S ACT 171 OF 2018 DATA BROKER REGULATION 14 (Dec. 11, 2018), http://bit.ly/2LZC3dj.

138. VT. STAT. ANN. tit. 9, § 2430(4)(A) (2018).

139. *Id.* § 2430(4)(B).

140. *Id.* § 2430(1)(A).

141. *Id.* § 2430(1)(A)(ix).

reasonably be used to identify a person constitutes personal information.[142] Publicly available information that is related to a consumer's business or profession is specifically excluded from being considered personal information.[143]

The Vermont law expressly prohibits the acquisition of consumers' personal information through fraudulent means as well as acquiring personal data for certain uses, including "engaging in unlawful discrimination."[144] The act authorizes individuals to sue entities that do not comply with its requirements through the cause of action created by the state's unfair and deceptive trade practices act.[145] Vermont's trade practices act authorizes courts to award compensatory damages, restitution, and attorney's fees to successful plaintiffs.[146] The state's Attorney General is also authorized to bring actions to enforce the act's provisions and can be awarded civil penalties of up to $10,000 per violation.[147]

Because insurance companies typically do not sell consumers' data to other parties it is unlikely that they will be considered data brokers under the Vermont statute. While this means that insurers will be exempt from the majority of the law's provisions, they could still be held liable for violations of its rules concerning prohibited uses of personal information.[148] The act does not explain what types of conduct constitute unlawful discrimination and the guidance document issued by the Attorney General only indicates that the term should be understood as it defined in other statutes and the state's common law.[149] This could leave the door open to insurers being sued by consumers under claims that the insurer acquired their personal information and used it in ways that led the insurer to treat members of protected classes worse than others.

IV. PART III - WHERE REGULATION FALLS SHORT & HOW NEW LAWS COULD PREVENT ANALYTICS ABUSE

Parts I and II identified how insurers' uses of Big Data analytics could harm individuals and discussed the laws regulating how commercial entities use consumer data. With this information established, it is possible to assess where existing regulations fail to sufficiently protect consumers' interests and proscribe additional actions. This Part begins by discussing

142. *See* VT. OFFICE OF ATT'Y GEN., *supra* note 137, at 5.
143. VT. STAT. ANN. tit. 9, § 2430(5)(B).
144. VT. STAT. ANN. tit. 9, § 2433(a)(1)–(2) (2018).
145. *Id.* § 2433(b)(1).
146. VT. STAT. ANN. tit. 9, § 2458 (2018).
147. *Id.*; VT. STAT. ANN. tit. 9, § 2433(b)(2).
148. *See* VT. OFFICE OF ATT'Y GEN., *supra* note 137, at 14.
149. *Id*. at 11.

how current laws could deter some insurers from compiling consumer data altogether, then takes a closer look at regulatory gaps in three areas of insurers' operations that will be most affected by analytics—marketing, underwriting, and claims management.

A. General Compliance Costs

One way that existing laws may succeed in limiting the use of Big Data analytics in consumer insurance is by imposing substantial compliance costs on companies that collect consumer data. While the FCRA, CCPA, and other data regulation laws do not directly charge companies substantial amounts to use consumer data, complying with the requirements set forth in these statutes may create large indirect costs for insurers. If compliance is expensive enough, it may become more efficient for insurance companies to forego consumer data analytics altogether.

Will existing laws impose substantial enough costs to deter insurers? Laws that focus exclusively on regulating data brokers like the Vermont Data Broker Act will not, as it is atypical for insurers to sell consumer data and, thus, they will not qualify as brokers. The primary compliance costs created by the Fair Credit Reporting Act are imposed on entities that constitute consumer reporting agencies, not insurers. Insurers must, however, maintain internal systems to make sure that they issue FCRA-required adverse action notices when they make certain types of underwriting decisions based on information purchased from consumer reporting agencies.[150] Insurers already have measures in place to satisfy these requirements, FCRA-related compliance costs should be minimal.

The California Consumer Privacy Act is the law that will create the largest compliance costs for insurers that use consumer data. Insurers that do business in California are highly likely to qualify as "businesses" within the regulation's scope.[151] The CCPA will force insurers to take actions that will enable them to comply with the law's notification, disclosure, and data security requirements. While the costs associated with instituting these measures is not publicly known, they are likely to be substantial.

Because of the potentially massive financial benefits that could come from the use of consumer-focused analytics, it seems unlikely that general compliance costs will be enough to deter insurers. The industry has such an established interest in pursuing analytics that additional reforms that merely add to these costs—for example, adopting a federal version of the CCPA or requiring all businesses to provide consumers with a right to deletion—would not dissuade them. Rather than attempt to use general

150. *See supra* Section II.A.
151. *See supra* Section II.B.

compliance requirements to dissuade insurers from using consumer data, the better approach will be to adopt rules that target the specific acts deemed to be abusive.

B. Marketing

There is very little in existing statutes that will have an impact on how insurers incorporate analytics into their marketing operations. As highlighted previously, this is significant because insurers will be able to use analytics-informed marketing practices to manipulate who becomes aware of their products and enters their applicant pool.[152] Not only will this increase the risk that it will be harder for disadvantaged communities to access insurance, but it could also enable them to indirectly reduce the number of members of certain protected classes from their policyholder pool.[153]

While the FCRA does impose some requirements on insurers that seek to use consumers' data for marketing purposes, these provisions will not prevent these potential harms. The biggest problem with the FCRA's rules in this context is that they will only limit an insurer's actions if they are using information from a credit reporting agency. Because data brokers have not been considered to be credit reporting agencies unless they provide credit scores, insurers can avoid all of the FCRA's marketing restrictions by either purchasing data from non-CRA brokers or gathering consumer data themselves.

Similarly, the CCPA is unlikely to significantly affect insurers employing analytics-informed marketing practices. The California law's primary mechanisms for giving consumers control over their data are simply a poor fit for these issues. Because insurers are likely to purchase consumer data from third-parties, they will not be required to issue disclosures directly to individuals and, hence, most individuals will not know whether an insurer is using their data to determine whether or not to market products to them. This lack of knowledge will also prevent consumers from effectively exercising their right to deletion. Realistically, the only CCPA-related mechanism that could prevent analytics-driven marketing practices is if consumers refuse to allow data brokers to sell their information, cutting insurers off from their primary source of data.

Given that the Vermont Data Broker Act does not target insurers, it is perhaps surprising that it may be the law that poses the most substantial threat to the use of consumer data in marketing. While the law primarily regulates the conduct of data brokers, it contains a broad prohibition on

152. *See supra* Section I.A.1.
153. *See supra* Section I.A.1.

any commercial entity procuring consumer data if it is going to use that information in a way that is unlawfully discriminatory.[154] As noted earlier, however, it is not clear which types (if any) of selective advertising practices may violate existing anti-discrimination laws.

There are no easy regulatory solutions for the problems associated with selective marketing. One approach would be to bar insurers from using analytics-informed means for targeting their advertisements altogether. This, however, would cause substantial problems for insurance companies in the world of digital advertising, where data-driven algorithms select practically all of the advertisements that consumers view. A better approach would be for insurance regulators to take steps to ensure that, regardless of the particular advertising practices an insurer employs, the company has a diverse applicant pool. Focusing regulatory requirements on the composition of insurers' applicant pools would permit companies the freedom to experiment with new advertising practices, while also providing the state a mechanism to ensure that vulnerable populations are not being ignored.

C. Underwriting

It is clear that each of the regulations discussed earlier will have some effect on insurers' underwriting practices. What is unclear is whether the impediments created by these statutes will be sufficient to prevent insurers from delegating underwriting processes to AI-controlled algorithms. Ideally, the rules placed on insurers' operations would allow computer-driven decision-making that improves the actuarial fairness of the company's actions, so long as those procedures do not impinge on autonomy, fairness, and other societal norms.

The FCRA explicitly authorizes insurers to purchase consumer data from credit reporting agencies and use this data when making underwriting decisions. The rights that the act provides to consumers—the right to notification of adverse action, the right to review and correct credit reporting agency's incorrect records—do not impose any direct limits on how insurers use their data. So long as an insurer's underwriting procedures allow the company to determine when it needs to issue an adverse action notice to consumers, the FCRA does not regulate the process the company uses to determine an individual's eligibility for insurance. Additionally, the FCRA places no limitations on insurers' procurement and use of data if the information comes from a non-credit reporting agency source, such as non-CRA data brokers or insurers' own

154. *See supra* Section II.C.

data collection efforts. Because of this, insurers will essentially always have the ability to opt-out of the FCRA's rules.

Whether the CCPA affects insurers' use of analytics in underwriting will largely depend on how some of its most ambiguous provisions are construed. On its face, the act's right to deletion provides a powerful mechanism for preventing the problems identified earlier. If consumers were able to force insurers to delete any information about the consumer that the insurer purchased from a broker, then insurers would be limited to looking at data the insurer collected directly from the consumer when making underwriting decisions. This would mean that insurers' practices would look more like those used before the Big Data era. The CCPA, however, states that businesses do not have to comply with an individual's request for deletion in a number of situations. Insurers faced with such requests will likely claim that they can keep consumers' data because they are using it in ways "that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business."[155] The resolution of disputes about the applicability of this exception will be a major determining factor of whether the CCPA plays a large role in insurers' underwriting operations. The extent to which consumers' exercise their rights to prevent data brokers from selling their data to insurers will also be important.

Finally, it is possible that the Vermont Data Broker Act's broad prohibition on the collection of consumer data for unlawfully discriminatory uses could affect insurers' underwriting practices. Until this provision's scope has been clarified, it is uncertain what standard will be used to determine whether insurance companies' underwriting practices constitute unlawful discrimination.

Given that none of the existing data use laws are likely to serve as substantial barriers to abusive algorithm-driven underwriting, additional regulation of insurers is necessary. The primary harms associated with insurers adopting a Big Data approach were that policyholders could be harmed if: decisions are made on the basis of correlations that seem tangential to the insured risks; preferential treatment is awarded based on immutable or luck-based characteristics; and insurers overreach when creating behavioral requirements for policyholders. All of these problems could be directly addressed through widespread adoption of regulatory measures that already exist in the insurance sphere.

The most direct way to resolve concerns that insurance companies' underwriting decisions will be based on specious correlations or criteria that unfairly disadvantage members of certain groups is to assert control over the factors that insurers are permitted to consider. Regulators have

155. CAL. CIV. CODE § 1798.105(d)(7) (West 2019).

developed two different approaches for doing this. First, there is the community rating approach, where a regulatory body determines a list of characteristics that insurers are allowed to consider when underwriting. Second, there is the file for approval approach, where insurers have to report the factors that it wants to base its underwriting decisions on to a regulatory body and receive its approval before doing so. Either of these approaches could effectively address both concerns by providing a safeguard against unfair decision-making processes.

Similarly, the best way to deal with concerns about insurers using insurability criteria to control consumers' behaviors is to require that insurers receive the approval of a regulator before adding coverage conditions to their policies. Many states already require insurers to submit their policy forms to a state body for approval.[156] Existing procedures could be modified to ensure that insurers disclose not only any coverage limitations added to their forms, but any other requirements that applicants must satisfy to be offered a policy.

D. Claims Management

Similar to how regulations do not currently constrain insurers' marketing practices, existing data use laws do not impose meaningful restraints on insurers' claims management practices. Aside from laws that prohibit unfair commercial conduct generally and proscribe bad faith actions by insurers, the state has not taken actions to prevent insurers from using unfair procedures for handling policyholders' claims. New rules need to be implemented to make sure that companies are not strategically denying or undervaluing the claims of vulnerable individuals.

The only limit that the FCRA places on insurers' use of consumer data in claims management is its general prohibition against using data from credit reporting agencies for non-approved purposes. The law does not restrict insurers' ability to use data procured from non-credit reporting agencies for any purposes.

The impact that the CCPA & Vermont Data Broker Act have on claims management practices will depend on the same factors identified in the prior section. If the exceptions to consumers' right to deletion are construed expansively, then the CCPA will not limit insurers ability to use individuals' when determining how to respond to their claims. Similarly, if individuals do not exercise their right to prevent brokers from selling

156. While it appears as though few state regulators actually conduct substantive reviews of submitted policies, measures could be adopted to ensure that meaningful review occurs. *See* Christopher C. French, *Understanding Insurance Policies as Noncontracts: An Alternative Approach to Drafting and Construing These Unique Financial Instruments*, 89 TEMP. L. REV. 535, 553 (2017).

their personal data, then the CCPA will not impair insurers' access to consumer data. The Vermont Data Broker Act's potential to limit insurers' ability to use consumer data in their operations depends on how its antidiscrimination provision is interpreted and enforced.

A straightforward bar on insurers using consumers' personal information when processing a claim seems like the ideal way to prevent the abuse of data analytics in the area of claims management. Once an insurer receives a claim under one of its policies, it is often clear what type of information will be relevant in determining whether the claim is covered or not. A rule that prohibits insurers from looking at any personal information the insurer possesses about the policyholder would effectively prevent insurers from profiling its policyholders and strategically denying claims. Given that some consumer information could be relevant to a coverage determination—e.g., the individual's GPS-derived location at the time of loss, the individual's purchase of accelerants the night of a fire—such a rule would need to include exceptions for data that insurers establish is directly linked to a claim.

V. CONCLUSION

It is clear that current statutes and regulations are not sufficient to prevent commercial entities from taking advantage of consumers. While it once appeared as though the Federal Trade Commission might serve as a force pushing for the regulation of consumer data,[157] there has been little indication in recent years that the federal government will take major action in this area. State legislatures in some states have begun to take up the mantle of data protection, but their efforts so far appear to be insufficient to address the concerns raised about the use of consumer data in insurance markets. In order to prevent insurers from engaging in unfair practices, state legislatures or regulatory bodies will need to enact rules that prohibit the specific behaviors identified in this Article.

157. *See generally* FTC, DATA BROKERS, *supra* note 34.