SECRET CONSUMER SCORES AND SEGMENTATIONS: SEPARATING "HAVES" FROM "HAVE-NOTS"

Amy J. Schmitz[*]

2014 MICH. ST. L. REV. 1411

ABSTRACT

"Big Data" is big business. Data brokers profit by tracking consumers' information and behavior both on- and offline and using this collected data to assign consumers evaluative scores and classify consumers into segments. Companies then use these consumer scores and segmentations for marketing and to determine what deals, offers, and remedies they provide to different individuals. These valuations and classifications are based on not only consumers' financial histories and relevant interests, but also their race, gender, ZIP Code, social status, education, familial ties, and a wide range of additional data. Nonetheless, consumers are largely unaware of these scores and segmentations, and generally have no way to challenge their veracity because they usually fall outside the purview of the Fair Credit Reporting Act (FCRA). Moreover, companies' use of these data devices may foster discrimination and augment preexisting power imbalances among consumers by funneling the best deals and remedies to the wealthiest and most sophisticated consumers. Use of these scores and segmentations increases the growing gap between powerful "haves" and vulnerable "have-nots." This Article sheds light on these data devices and aims to spark adoption of data privacy regulations that protect all consumers regardless of their educational, economic, ethnic, or social status.

---

* Amy J. Schmitz, Professor of Law, University of Colorado School of Law. I thank Kristen Carpenter, Paul Ohm, and Blake Reid for their helpful comments, and Megan Coontz McAllister, Laurence Gendelman, Mary Sue Greenleaf, and Danyelle McNeary for their insights and research assistance. Related research was funded in part by the Implementation of Multicultural Perspectives and Approaches in Research and Teaching (IMPART) Awards Program.

TABLE OF CONTENTS

INTRODUCTION

Data brokers collect and sell information about consumers to companies for marketing and other purposes. This is not a surprise to most consumers. The media is filled with stories about "Big Data" and rising concerns with online privacy. What may be surprising to many, however, is the breadth and depth of data collection and the secret ways companies use this information to categorize, evaluate, and essentially discriminate among consumers.[1] Data brokers gather

1. *See* EDITH RAMIREZ ET AL., FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY i-ix (2014), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.

not only consumers' spending and debt histories, but also much more intimate details of consumers' financial, social, and personal lives. They track where consumers shop, what they shop for, how they pay for purchases, and much more. Some data brokers even make assumptions about consumers based on whether they use a pen or pencil to fill out forms.[2]

Data sharing and aggregation also have reached unimaginable levels. Data brokers share and sell information among themselves through a complex web of relationships to create individual and group-based consumer files. These files include a vast array of data points from online and offline sources. The Federal Trade Commission (FTC) found in its 2014 study of the largest data brokers that one broker had "information on 1.4 billion consumer transactions and over 700 billion aggregated data elements," and another broker "adds three billion new records each month to its databases."[3] Furthermore, one of the studied brokers "has 3000 data segments for nearly every U.S. consumer."[4]

Data brokers use this mammoth amount of information to predict consumer behavior and propensities. They make assumptions and inferences based on the information collected to classify consumers into segments for positive and negative marketing campaigns. For example, brokers have generated marketing lists for pet stores based on consumers' dog product purchasing histories, in an effort to help these stores target those who would likely want their products.[5] However, brokers also have used collected data indicating low income combined with Latino or African-American descent to classify consumers into segments under seemingly innocuous labels such as "Urban Scramble" and "Mobile Mixers," possibly fueling exploitative marketing to these individuals.[6]

---

pdf?utm_source=govdelivery; *see also* Katy Bachman, *Consumer Scores Are the Next Privacy Boogeyman in Washington: Report Details 'Hundreds of Secret Consumer Scores,'* ADWEEK (Apr. 3, 2014, 12:47 PM), http://www.adweek.com/news/technology/consumer-scores-are-next-privacy-boogeyman-washington-156753 (emphasizing the secret nature of these consumer scores with power to determine our financial futures in today's market).

2. *See* Nathalie Martin, *Hey Dude, What's Your E-score*, CREDIT SLIPS (Aug. 20, 2012, 1:02 PM), http://www.creditslips.org/creditslips/2012/08/hey-dude-whats-your-e-score.html.

3. RAMIREZ ET AL., *supra* note 1, at iv, 46-47 (encapsulating the FTC's findings).

4. *Id.* at iv, 47.

5. *See id.* at 47.

6. *Id.* (internal quotation marks omitted).

In addition, some data brokers go beyond consumer segmentation to create logarithmic consumer "scores" or ratings that they sell to companies for marketing and other purposes.[7] Companies use these predictive segmentations and scores to assess each consumer's likely value to the company and to decide what offers and remedies each consumer deserves in the company's assessment.[8] A consumer's score may thus inform how a company will treat that individual when he or she calls customer service or asks about the company's products and services.[9]

Consumer segmentations and scores therefore have powerful impacts.[10] Companies may use such predictive data devices to discriminate against consumers they deem less valuable or too risky. A New York Times reporter observed:

> A growing number of companies, including banks, credit and debit card providers, insurers and online educational institutions are using these scores to choose whom to woo on the Web. These scores can determine whether someone is pitched a platinum credit card or a plain one, a full-service cable plan or none at all. They can determine whether a customer is routed promptly to an attentive service agent or relegated to an overflow call center.[11]

Despite this power, these scores are largely secret and impossible to decipher without an in-depth understanding of data analytics.[12] Businesses guard information about consumer scores as

---

7. PAM DIXON & ROBERT GELLMAN, THE SCORING OF AMERICA: HOW SECRET CONSUMER SCORES THREATEN YOUR PRIVACY AND YOUR FUTURE 6-10 (2014), *available at* http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf.

8. *See id.* at 19-20 (discussing the different uses of consumer scores).

9. Natasha Singer, *Secret E-Scores Chart Consumers' Buying Power*, N.Y. TIMES (Aug. 18, 2012), http://www.nytimes.com/2012/08/19/business/electronic-scores-rank-consumers-by-potential-value.html?pagewanted=all&_r=0.

10. *See* Ariel Porat & Lior Jacob Strahilevitz, *Personalizing Default Rules and Disclosure with Big Data*, 112 MICH. L. REV. 1417, 1440 (2014) ("Big Data can be used to predict future behavior because the process of studying an individual's purchases, online searches, borrowing activity, and social network composition reveals aspects of that individual's personality and preferences.").

11. Singer, *supra* note 9.

12. *See* 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, 855-67 (2013). Professor Nathalie Martin commented that "[t]he e-score process is entirely nontransparent and obviously not regulated." Martin, *supra* note 2.

proprietary trade secrets.[13] They also generally have no legal duty to comply with credit reporting rules with respect to these ratings and scores because they are not used for determining credit, insurance, or employment per se.[14] Instead, companies assert that they use these predictive valuations and classifications for marketing, which is merely benign business in our capitalist economy.[15]

Use of consumer data also seems fair to the extent that it rewards consumers for positive purchasing and payment histories, and funnels offers to consumers to suit their interests. It also may allow companies to save money by targeting their marketing and retention efforts. They theoretically can then pass on their cost savings to consumers through lower prices and higher quality goods and services. At the same time, companies may seek only the customers they deem most lucrative. Furthermore, "price discrimination, in the sense of price differences unsupported by cost differences," is common.[16]

Nonetheless, price differentials based on consumer ratings perpetuate cycles of poverty.[17] They augment power imbalances between the economically and socially powerful "haves" and the disempowered "have-nots."[18] For example, consumers with more education and higher income, and those who live in prestigious neighborhoods, are likely to have more favorable consumer scores or profiles—and thus obtain better offers, deals, and overall treatment.[19] Consumers also may receive special remedies because they have

---

13. Brenda Reddix-Smalls, *Credit Scoring and Trade Secrecy: An Algorithmic Quagmire or How the Lack of Transparency in Complex Financial Models Scuttled the Finance Market*, 12 U.C. DAVIS BUS. L.J. 87, 117-18 (2011).

14. *See* Fair Credit Reporting Act, 15 U.S.C. § 1681t(b) (2012) (indicating the narrow parameters of the Act, which do not extend to general data collection and reporting for marketing purposes).

15. *See* DIXON & GELLMAN, *supra* note 7, at 20 ("In new consumer scoring, some have argued that the scores are mainly just for marketing and are largely beneficial.").

16. Michael E. Levine, *Price Discrimination Without Market Power*, 19 YALE J. ON REG. 1, 8 (2002).

17. *See, e.g.*, R. Ted Cruz & Jeffrey J. Hinck, *Not My Brother's Keeper: The Inability of an Informed Minority to Correct for Imperfect Information*, 47 HASTINGS L.J. 635, 672-76 (1996) (discussing how sellers differentiate among buyers by providing contract changes and adjustments to only the most sophisticated consumers who complain).

18. *See generally* Amy J. Schmitz, *Access to Consumer Remedies in the Squeaky Wheel System*, 39 PEPP. L. REV. 279 (2012).

19. *See* Nate Cullerton, Note, *Behavioral Credit Scoring*, 101 GEO. L.J. 807, 820-24 (discussing the discriminatory dynamics regarding data collection).

higher social capital based on their propensity to post on social media and gather followers and friends online.[20] Meanwhile, less powerful or socially savvy consumers may miss out on these deals and perks.[21] Moreover, scores and segmentations that factor in race, gender, and other suspect considerations may foster discrimination.[22]

At the same time, lack of transparency regarding consumer scores and segmentations stymies proper market regulation. It prevents economists' theoretical "informed minority" from learning about or notifying others of unfair practices and threatening to go elsewhere if companies do not make appropriate changes.[23] First, there is no evidence that a sufficient number of "informed" consumers know their rights or read privacy policies, especially when the terms may not be easily accessible or easy to understand.[24] Furthermore, even if some "informed minority" exists, only a handful of these consumers contest use of their information or seek better deals.[25] In addition, individuals who receive better deals have little to no incentive to share information about rationed benefits

20. *See* RAMIREZ ET AL., *supra* note 1, at 31.

21. *See* Schmitz, *supra* note 18, at 296-300.

22. *See* Cullerton, *supra* note 19, at 808 (discussing the heightened potential of discrimination facilitated by data collection).

23. *See* Alan Schwartz & Louis L. Wilde, *Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic Analysis*, 127 U. PA. L. REV. 630, 637-39 (1979) ("Thus, if enough searchers exist, firms have incentives both to compete for their business and to offer the same terms to nonsearchers. When the preferences of searchers are positively correlated with the preferences of nonsearchers, competition among firms for searchers should tend to protect all consumers.").

24. *See* Cruz & Hinck, *supra* note 17, at 664-76 (concluding that the informed minority argument is based on faulty assumptions); Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts* 1-26 (N.Y. Univ. Law & Econ. Research Paper Series, Working Paper No. 09-40, 2009), *available at* http://ssrn.com/abstract=1443256 (studying the Internet browsing of 48,154 households and finding that only one or two in 1,000 shoppers studied online software merchants or accessed their websites). Even proactive shoppers usually focus on only price and a few other terms particular to their needs. LARRY A. DIMATTEO ET AL., VISIONS OF CONTRACT THEORY: RATIONALITY, BARGAINING, AND INTERPRETATION 29 (2007).

25. *See* Cruz & Hinck, *supra* note 17, at 647-50 (explaining and questioning the informed minority argument); Lee Goldman, *My Way and the Highway: The Law and Economics of Choice of Forum Clauses in Consumer Form Contracts*, 86 NW. U. L. REV. 700, 714-16 (1992) (explaining the informed minority argument through a discussion of the "marginal set of informed consumers").

with the uninformed masses.[26] Businesses then continue to manipulate contract terms and hide use of consumer data under the guise of "marketing" and proprietary business practices beyond the scope of credit reporting rules.[27]

Additionally, the lack of personal relations and shared contract understandings in Business-to-Consumer (B2C) exchanges augment concerns with consumer scoring and segmentation.[28] Companies often have no basis besides data brokers' predictions to decipher which consumers they should seek or retain. Scores and segments based on economic and noneconomic factors create easy rubrics for discriminating among consumers, while lack of transparency denies consumers the opportunity to challenge the veracity of these valuations or alert others to risks associated with these assessments. Meanwhile, data brokers become more and more sophisticated in uncovering and manipulating consumers' behavioral propensities.[29] In summary, this creates a strong need for consumer protections that a broken market has failed to provide.

The FTC highlighted these concerns regarding Big Data's collection and use of consumer data in its May 2014 report, and has urged Congress to take action to protect consumers' data privacy.[30] The FTC and the White House have urged data brokers to provide consumers with clear notice and increased choice with respect to collection and use of personal data.[31] Some commentators and policymakers also have proposed that the Fair Credit Reporting Act (FCRA), which is applicable to data reports used for credit, insurance, and employment determinations, should be extended to

---

26. *See* Peter A. Alces & Jason M. Hopkins, *Carrying a Good Joke Too Far*, 83 CHI.-KENT L. REV. 879, 895-97 (2008) (discussing how businesses may discriminate in favor of sophisticated consumers by reducing fees and foregoing enforcement of terms in their form agreements that are otherwise "prejudicial to customer interests").

27. *See infra* notes 89, 98 and accompanying text.

28. Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1003-04 (2014).

29. *See id.*

30. RAMIREZ ET AL., *supra* note 1, at 49.

31. Alexei Alexis, *Big Data Report to Obama Urges Reforms on Breach Notice, ECPA, Consumer Rights*, BLOOMBERG BNA (May 5, 2014), http://www.bna.com/big-data-report-n17179890156/ (urging advancement of the Obama administration's proposed privacy "bill of rights" and data security breach notification legislation); RAMIREZ ET AL., *supra* note 1, at 46-57 (recommending legislation and policies to increase consumers' access to information about data collected and to opt out of allowing for use of their data).

cover consumer scoring more generally.[32] However, the FCRA has not been entirely effective, and it is uncertain whether and how it should apply to other consumer scores.[33]

Accordingly, this Article seeks to shed light on consumer scores and segmentations, and present suggestions for regulating these data devices with an eye toward maximizing their benefits and minimizing their drawbacks and dangers. Indeed, the time is ripe for such regulation, as the FTC is examining the effects of Big Data on low income and underserved consumers.[34] Furthermore, the Consumer Financial Protection Bureau (CFPB), created by Dodd–Frank Wall Street Reform and Consumer Protection Act (Dodd–Frank), has voiced concern regarding consumer privacy with respect to financial products and services.[35]

Part I of this Article depicts the depth and breadth of data collection and the use of this data to score and classify consumers for marketing and other purposes. Part II then discusses the current laws and regulations that may apply to data collection, as well as rules restricting data reporting with respect to mainly credit, insurance, and employment decisions. In light of the current laws' limitations, Part III considers the FTC's and others' proposals for regulations and reforms aimed to protect consumers from the dangers of rampant data collection, scoring, and segmentation. It also highlights the promise and pitfalls of these proposals and provides suggestions for balanced reforms that address how such data practices contribute to the growing gap between consumer "haves" and "have-nots." The Article concludes by inviting policymakers, businesses, and consumer groups to consider these and other ideas for imposing just and cost-effective restrictions on Big Data.

---

32. Fair Credit Reporting Act, 15 U.S.C. § 1681a(d)(1) (2012).

33. *See* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 5 (2014).

34. *FTC to Examine Effects of Big Data on Low Income and Underserved Consumers at September Workshop*, FED. TRADE COMMISSION (Apr. 11, 2014), http://www.ftc.gov/news-events/press-releases/2014/04/ftc-examine-effects-big-data-low-income-underserved-consumers (announcing the September 2014 workshop to explore these issues).

35. Dodd–Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376, 1964 (2010) [hereinafter Dodd–Frank]; David Cho & Michael D. Shear, *White House Issues Detailed Proposal for Consumer-Finance Watchdog*, WASH. POST (July 1, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/06/30/AR2009063004187.html.

I. CONSUMER SCORES AND SEGMENTATIONS IN THE EXPANDING WORLD OF BIG DATA

Data collection has expanded exponentially with the growth of the Internet and online contracting, and data brokers have banked on that growth in selling consumers' information. Furthermore, brokers have plugged that data into highly technical algorithms to create consumer classifications and scores or ratings that companies then use to determine how they will treat consumers in the marketplace. Such assessments based on collected data and inferences may benefit companies and consumers when they enhance products and services, and open doors to positive innovations. However, such expansion of Big Data has become problematic due to its clandestine nature and discriminatory effects.[36]

A. Expanding Data-Broker Industry

Data collection is not new. The United States Census Bureau has been gathering data since the first census in 1790.[37] Since that time, however, privacy concerns have risen exponentially as not only the government, but also private companies and data brokers gather information about consumers from both online and offline sources.[38] The news is filled with stories of data breaches and identity theft. This has created growing angst among consumers in the online marketplace, with 92% of U.S. Internet users worrying about their online privacy.[39]

Nonetheless, consumers are not fully aware of the depth and breadth of data collection and online tracking by private companies operating outside of the public eye. Only 47% of respondents in that

---

36. *See* Cullerton, *supra* note 19, at 808. Notably, lack of consumer privacy protections in the United States also has had significant impacts on national and economic security. *See* LAURA K. DONOHUE, HIGH TECHNOLOGY, CONSUMER PRIVACY, AND U.S. NATIONAL SECURITY (2014) (providing written remarks for the U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade). This reinforces the need for better consumer privacy protections in the United States and should hasten policymakers' efforts in that regard.

37. *Agency History*, U.S. CENSUS BUREAU, http://www.census.gov/history/www/census_then_now/ (last visited Jan. 7, 2015).

38. *See* RAMIREZ ET AL., *supra* note 1, at 49.

39. *See* TRUSTE, TRUSTE 2014 US CONSUMER CONFIDENCE PRIVACY REPORT: CONSUMER OPINION AND BUSINESS IMPACT 3 (2014), *available at* http://download.truste.com/dload.php/?f=4HKV87KT-447.

same survey of Internet users said they were concerned with companies tracking their behavior online.[40] In reality, however, all consumers have good reason to be very concerned with the expanse of Big Data and its tracking tirade. As noted above, the FTC found that data brokers gather information on billions of transactions and aggregate hundreds of billions of data elements to create consumer profiles.[41]

Search engines like Google, Yahoo, and Bing are notorious for collecting consumers' data.[42] EBay, Amazon, ESPN, Disney (which owns ABC), MySpace, Facebook, YouTube, and Twitter are just a handful of the companies that eagerly collect their patrons' data and searching habits.[43] Furthermore, companies such as IBM, which were once associated with computer products and software, have moved into the data industry, viewing data as "the world's new natural resource."[44] Consumers should expect that Internet Service Providers (ISPs), search engines, merchants, and other data brokers are tracking their every move online.[45]

This increase in "who" collects data pales in comparison to the mammoth expansion in "what" data companies collect about consumers. Data collectors track consumers when they make online purchases, use store loyalty cards, and pay for goods or services using their credit and debit cards.[46] They also track spending habits, how long one lingers on a website, consumers' online searching histories, family information, and even postings on social sites such as Facebook.[47] "Consumer data companies are scooping up huge

---

40. *Id.* at 3-6. Nonetheless, concerns about tracking have escalated among those aged 55-64, and is higher among married than single persons. *Id.* at 7.

41. *See* RAMIREZ ET AL., *supra* note 1, at 46-47.

42. *See* Mierzwinski & Chester, *supra* note 12, at 847.

43. Joseph Conlin, *The New Media and Marketing Landscape*, at *7 (Jan. 29, 2014), https://web.archive.org/web/20140815012524/http://www1bpt.bridgeport.edu/~jconlin/InternetMarketing.pdf.

44. IBM, WHAT WILL WE MAKE OF THIS MOMENT? 2013 IBM ANNUAL REPORT 13-15 (2013), *available at* http://www.ibm.com/annualreport/2013/bin/assets/2013_ibm_annual.pdf (focusing strategy on transforming IBM's place in Big Data for prediction and prescription based on collected and aggregated data).

45. *See Online Information Brokers and Your Privacy*, PRIVACY RIGHTS CLEARINGHOUSE (Oct. 1, 2004), https://www.privacyrights.org/print/ar/infobrokers.htm.

46. *See What Information Do Data Brokers Have On Consumers, and How Do They Use It: Hearing Before the S. Comm. on Commerce, Sci., & Transp.*, 113th Cong. 9 (2013) (statement of Jessica Rich, Director of the Bureau of Consumer Protection of the Federal Trade Commission).

47. *See* Conlin, *supra* note 43.

amounts of consumer information" and "selling it, providing marketers details about whether you're pregnant or divorced or trying to lose weight, about how rich you are and what kinds of cars you drive."[48]

Data brokers also augment information with data from one's ISP, device-tracking software, facial recognition software, and programs like Google AdSense in order to build consumer profiles.[49] This may include information about consumers' use of particular browsers, propensity to click on certain ads, phone numbers, email address, location, IP address, and much more.[50] Data brokers also have become especially vigilant in tracking consumers' third-party and social connections online. Indeed, data collection and aggregation transpires through an unimaginable labyrinth of information sharing among merchants and data brokers.[51]

"Cookies" may not be so sweet to consumers. Cookies, embedded in almost all websites, track consumers while navigating a website, and may follow the consumer's activity to gather further information as he or she visits other websites.[52] These cookies are usually stealth. However, one can see what bluekai.com, for example, has gathered from some cookies by visiting http://www.bluekai.com/registry.[53] Such rare disclosures are somewhat refreshing, but equally alarming for many consumers.[54]

Researchers at the University of California, Berkeley compared top websites' cookies and other tracking technologies from 2009 to 2011 with tracking technologies in 2013 and found that "the number

---

48. Lois Beckett, *Everything We Know About What Data Brokers Know About You*, PROPUBLICA (June 13, 2014, 12:59 PM), http://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you.

49. Bono, *'Reclaim Your Name:' Find Out What Big Data Companies Know About You*, SKYTECHGEEK (Aug. 2, 2013), http://web.archive.org/web/20140702075145/http://skytechgeek.com/2013/08/big-data-companies-know-about-you/.

50. *Id.*; *see also*, Laura J. Bowman, Note, *Pulling Back the Curtain: Online Consumer Tracking*, 7 ISJLP 721, 727, 733-36, 748-49 (2012).

51. *See generally* Andrew W. Bagley & Justin S. Brown, Consumer Legal Protections Against the Layers of Big Data (unpublished manuscript) (2014 TPRC Conference Paper), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418805##.

52. *See* RAMIREZ ET AL., *supra* note 1, at 29-30 (discussing the use of cookies).

53. *The Bluekai Registry—Putting Consumers in Control of Their Digital Footprint*, ORACLE: BLUEKAI, http://www.bluekai.com/registry/ (last visited Jan. 7, 2015).

54. It caused quite a stir when I had students in one of my classes check their names on this site.

of tracking cookies expanded dramatically[,] and . . . advertisers had developed new, previously unobserved tracking mechanisms that users cannot avoid even with the strongest privacy settings."[55] They found that 100% of the top websites now use tracking software and that third-party tracking companies and advertisers, instead of first-party sites, now place most cookies without consumers' approval or awareness.[56]

Tracking can be quite extensive. For example, Bloomberg News reporters gained access to every aspect of users' research information on the Bloomberg Terminal.[57] The intricacies of the tracking allowed these reporters to track users' every keystroke.[58] One commentator likened this data collection through Bloomberg Terminal as a modern equivalent of the "memex" 1945 futuristic concept of a desktop technology that records trails of searches and other information for later users.[59] The commentator also argued that so-called "[d]eidentification" of data as a safeguard for user privacy is largely ineffective because IP addresses and other identifying information can easily be reattached to ostensibly anonymous user data.[60]

While consumers may enjoy the personalized advertisements they receive due to tracking, they are often alarmed that they are unable to easily block data tracking.[61] Many data brokers do not offer a method for opting out of data sharing.[62] Moreover, consumers unknowingly may consent to share data with layers of data collectors

---

55. Chris Jay Hoofnagle et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L & POL'Y REV. 273, 273 (2012). A *Wall Street Journal* article found that the "nation's 50 top websites on average installed 64 pieces of tracking technology onto the computers of visitors, usually with no warning." Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., July 31, 2010, at W1.

56. Hoofnagle et al., *supra* note 55, at 276.

57. *See* James Grimmelmann, *Big Data's Other Privacy Problem* 2-3 (Univ. of Md. Francis King Carey Sch. of Law, Paper No. 7, 2014), *available at* http://ssrn.com/abstract=2358079.

58. *Id.*

59. *Id.* at 1.

60. *Id.* at 6.

61. *See id.* at 2-5.

62. *See* Erica M. Scott, Note, *Protecting Consumer Data While Allowing the Web to Develop Self-Sustaining Architecture: Is a Trans-Atlantic Browser-Based Opt-In for Behavioral Tracking the Right Solution?*, 1 PAC. MCGEORGE GLOBAL BUS. & DEV. L. J. 285, 295-305 (2014); Julia Angwin, *Privacy Tools: Opting Out from Data Brokers*, PROPUBLICA (Jan. 30, 2014, 1:29 PM), http://www.propublica.org/article/privacy-tools-opting-out-from-data-brokers.

by failing to opt out of data collection and sharing with one company.[63] The FTC found that because data brokers are usually not consumer-facing, it is confusing or nearly impossible for consumers to opt out of data collection and sharing even when data brokers ostensibly provide that option.[64] Furthermore, even the sophisticated and informed minority of consumers that learn about and access brokers' websites that do allow for opting out may not realize the limitations of those opt-outs or that doing so with one company will not protect against other companies' data mining.[65]

Consumers also are slow to block cookies when searching the web because companies often state that site features are not available without cookies enabled.[66] Advertisers have agreed "in principle to a universal 'Do Not Track' mechanism," but that does not preclude third parties including Google, Facebook, and others from continuing to gather data via cookies and other tracking mechanisms.[67] In addition, removed information "may be re-posted . . . at a later date when [a] company downloads a new batch of information."[68] Robust tracking mechanisms such as "Flash cookies" also gather increasingly more information and can reinstate themselves after being deleted.[69]

Furthermore, data collectors and merchants benefit by offering "free" online services.[70] The problem is that "free" is not truly free.[71] For example, some websites provide consumers with "free" rate calculators and other online tools to gather quotes and information

---

63. Bagley & Brown, *supra* note 51, at 33-40.

64. RAMIREZ ET AL., *supra* note 1, at 49.

65. *Id.* at 49, 53 (noting that many data brokers do not provide consumers with access to their data with respect to risk mitigation products offered to help companies verify identity).

66. *See* Hoofnagle et al., *supra* note 55, at 290 (discussing how Hulu requires users to accept cookies to access certain services).

67. *Id.* at 275-76.

68. *Online Information Brokers and Your Privacy*, *supra* note 45 (stating further tips and information regarding data broker issues).

69. Hoofnagle et al., *supra* note 55, at 282. Similarly, technologies that write files to users' computers (Etags, Flash cookies, HTML5 local storage, and Evercookies) are also difficult to block and delete because they can reinstate themselves. *Id.* at 281-85. There are also technologies that rely on attributes of users' computers (i.e., using an aggregate of features such as browser type, plug-ins, and font) as a "fingerprint" to remotely track users' Internet usage based on what their computers do. *Id.*

70. Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 608 (2014).

71. *Id.* at 609.

for products such as mortgages, college loans, or insurance.[72] These fill-in-the-form search widgets assist consumers in their budgeting and in obtaining services ranging from finding home contractors to choosing car insurance and applying for online degrees.[73] Consumers seeking the information and assistance willingly divulge vast amounts of personal, financial, and even health information. Data brokers then use and sell this information gathered through these widgets.[74]

Data brokers also collect and share data from location-tracking services. The Government Accountability Office (GAO) studied in-car location services at the end of 2013 in an effort to understand the breadth and depth of the data issues associated with these services.[75] It asked ten companies that offer these location-based services regarding their use of collected data and associated policies.[76] It found that all of these companies collect location data, and nine of the ten share that data with third parties for the purpose of providing services to consumers.[77] Nonetheless, all of the companies said that they do not share or sell personally identifiable information or location data with data brokers, and they aim to comply with best practices such as disclosing their use of data to their customers.[78] However, the GAO also found that the companies' disclosures were often misleading, did not give consumers power to delete or safeguard their data, and failed to provide information on how the companies hold themselves and their employees accountable.[79]

Again, consumers may enjoy the benefits of widgets and the personalized advertisements that companies generate based on gathered information. However, data aggregation and sharing is deep and vast. This data includes information from various public records, online tracking, and monitoring in the physical world. Real estate, criminal, bankruptcy, and any other public records are all fair game for data collectors. Consumers' age, address, family data, ethnicity,

72. Mierzwinski & Chester, *supra* note 12, at 856.
73. *Id.*
74. Hoofnagle & Whittington, *supra* note 70, at 633.
75. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-14-81, IN-CAR LOCATION-BASED SERVICES: COMPANIES ARE TAKING STEPS TO PROTECT PRIVACY, BUT SOME RISKS MAY NOT BE CLEAR TO CONSUMERS (2013), *available at* http://www.gao.gov/products/GAO-14-81.
76. *Id.*
77. *Id.*
78. *Id.*
79. *Id.*

employment, and medical information also are easily accessible.[80] Data brokers also gather information through consumers' use of store loyalty cards and coupons, as well as entries to seemingly benign contests and raffles.[81] One company even adds its assumption that those who fill out forms using a pen instead of a pencil are more likely to pay their bills on time.[82] Moreover, downstream data aggregation makes it nearly impossible for consumers to determine where or how a particular company has obtained their data.[83]

Accordingly, data brokers' business model is essentially to gather as much information as possible and sell it to the highest bidders.[84] They use this data to create consumer profiles that inform how companies treat consumers in the marketplace.[85] Consumers are nonetheless unaware of this data collection and unable to verify the data's accuracy.[86] Inaccurate data and assumptions may then lead companies to offer consumers less or more advantageous deals than warranted.[87] Moreover, algorithmic determinations may incorporate discriminatory assumptions and perpetuate problematic stereotypes that hinder consumers seeking to overcome social and economic barriers.[88]

B. Secret Scoring and Segmentations of Consumers' Value

Boundaries have blurred between data collection and consumer scoring or valuation. Data brokers profit by selling leads and using

---

80. *See Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA*, FED. TRADE COMMISSION (June 12, 2012), http://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed.

81. *See What Information Do Data Brokers Have On Consumers, and How Do They Use It*, *supra* note 46, at 9.

82. Martin, *supra* note 2 (stating that a founder of a leading e-score company "learned working at Fingerhut how to sniff out a good paying customer, concluding . . . that people who filled out forms in pen were better payers than those who used pencils and people who used a middle initial paid more often that [sic] those who did not").

83. RAMIREZ ET AL., *supra* note 1, app. at C, C-7 (providing statements of Commissioner Julie Brill).

84. Angwin, *supra* note 55, at W1.

85. *Id.*

86. *See id.*

87. *See id.*; Howard Baldwin, *Big Data's Big Impact Across Industries*, FORBES (Mar. 28, 2014, 2:05 PM), http://www.forbes.com/sites/howardbaldwin/2014/03/28/big-datas-big-impact-across-industries/.

88. *See* Cullerton, *supra* note 19, at 820-24.

gathered data to differentiate among consumers. For example, Bankrate.com gathers data and generates leads that it sells to companies to enhance their marketing strategies.[89] Bankrate hosts a consumer-friendly website with rate calculators and other tools that prompt individuals to provide a wide array of personal and financial information in order to obtain loan- and insurance-rate quotes.[90] As noted above, such ostensibly "free" widgets can assist consumers in creating budgets and planning finances. As Bankrate.com boasts on its site, it is "the Web's leading aggregator of financial rate information" and "provides free rate information to consumers on more than 300 financial products" with the help of its staff of reporters and experts.[91] It also notes that it works with a network and co-branded sites to "provide the tools and information via a suite of products and services that can help consumers make better informed financial decisions."[92]

Despite the consumer-friendly nature of Bankrate.com, the site does not make it clear to consumers that it profits from collecting website visitors' personal contact information, device details, ISP data, and location.[93] Although Bankrate's privacy policy reveals that the company may transmit data collected about consumers to third parties, it does not explain that it also may sell the data for fees ranging from $8 for an insurance prospect and $35 for a finance lead to $75 for a mortgage prospect.[94] Researchers found that in 2011, for example, Bankrate.com sold 18 million leads to 20,000 agents and 75 carriers at considerable profits.[95] Bankrate.com also works with major, but little known, online scoring companies TARGUSinfo and eBureau to determine more precisely what it predicts as consumers' value to particular businesses.[96]

Bankrate.com is not alone in profiting from data collection and lead generation. Experian, for example, has branched well beyond

89. Singer, *supra* note 9; *see also About Bankrate*, BANKRATE, http://www.bankrate.com/coinfo/default.asp (highlighting that the site seeks to benefit consumers and not discussing the lead generation aspects beyond mention of "partners") (last visited Jan. 7, 2015).

90. *About Bankrate*, *supra* note 89.

91. *Id.*

92. *Id.*

93. *Privacy Policy*, BANKRATE, http://www.bankrate.com/coinfo/privacy.asp (last updated Sept. 17, 2014).

94. Singer, *supra* note 9; *see also* Mierzwinski & Chester, *supra* note 12, at 852 n.26.

95. Mierzwinski & Chester, *supra* note 12, at 857.

96. *Id.*

traditional credit reporting to sell leads.[97] Experian even sells lists of expectant parents and families with babies, who companies then target for marketing certain products.[98] Similarly, these data brokers may aggregate consumers' information from various sources and plug a wide variety of information into data-driven calculations and predictive models.[99] These decisional models theoretically seek to account for a holistic view of each customer in crafting scores and/or ratings that companies use to differentiate among consumers.[100]

Consumer scoring therefore takes data collection and lead generation to the next level by using complicated mathematics, statistical modeling, and algorithms to crystallize many factors into numbers companies may use for marketing, predicting future behavior, assessing risks, and essentially determining how they treat different consumers.[101] Consumer scoring companies employ actuaries and math wizards to essentially boil down a vast amount of data into scores or ratings that aim to predict an individual consumer's likely value as a customer.[102] These formulas and equations nonetheless remain a mystery to consumers because they are generally considered proprietary and shielded by trade secret law.[103]

EBureau is a leader in the consumer scoring industry.[104] This company markets "eScores" as "a service that enables rapid development and deployment of customized statistical scores" that enable companies to optimize marketing, accounts receivable management, and other important interactions with consumers.[105] It bases its scores on a "massive data warehouse" that includes consumer credit data, real property and asset records, household demographics, various files containing name, address, telephone and

97. Beckett, *supra* note 48.
98. *See id.*
99. Bagley & Brown, *supra* note 51, at 6.
100. DIXON & GELLMAN, *supra* note 7, at 8.
101. *Id.* at 6-10.
102. *Id.* at 27-28.
103. Reddix-Smalls, *supra* note 13, at 117-18. It is impossible for consumers to learn about or understand exactly what goes into their credit scores or whether they are statistically correct due to complicated algorithms. *Id.* Moreover, not even the government is able to pierce trade secrets law to test the algorithms' accuracy or validity. *Id.*
104. *About eBureau*, EBUREAU, http://www.ebureau.com (last visited Jan. 7, 2015).
105. EBUREAU, ESCORES DATA SHEET, *available at* http://www.ebureau.com/sites/all/files/file/datasheets/ebureau_escore_datasheet.pdf (last visited Jan. 7, 2015).

date of birth information, Internet and other purchase histories, bankruptcy filings, and other public documents.[106] It also may include behavioral assumptions in the mix of factors contributing to eScores.

EBureau's algorithms remain secret, but it does reveal that it adds several thousand details from its data warehouse to the data sets that clients submit from their current marketing lists.[107] EBureau then extrapolates common factors among these existing customer bases and uses that data to create complicated algorithms to determine prospective consumer eScores.[108] These scores range from zero to ninety-nine, with ninety-nine indicating the best and zero indicating the worst likely return on a company's investment.[109] EBureau highlights low scores as especially important in culling would-be customers.[110] In online education, for instance, schools use scores to winnow prospective students as not worth the investment of course catalogs or follow-up calls.[111]

In addition to eScores, eBureau also offers the following:

> eTarget Demographics, a real-time consumer demographic data append service that helps B2C online marketers to instantly gain a comprehensive perspective of their opt-in Website visitor; Income Estimator, a model-driven information append service that helps consumer-facing companies to estimate a person's income; and eLink, a service that helps accounts receivable management firms and departments locate, update, and append information to a debtor record.[112]

Essentially, eBureau not only gathers data, but also adds information from various sources to consumers' files and makes predictions that companies use in a wide variety of ways.

Data brokers like eBureau may provide companies with efficient marketing and workflow devices by helping them to best allocate marketing resources. However, the data and assumptions at the foundation of consumer scores may not be accurate. The FTC found in its study that although data brokers usually take some steps to check accuracy of data collected, data quality varies greatly

106. *Id.*
107. Singer, *supra* note 9.
108. *Id.*
109. *Id.*
110. *Id.*
111. *Id.*
112. *Company Overview of eBureau, LLC*, BLOOMBERG BUSINESSWEEK, http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapid=27128128 (last visited Jan. 7, 2015).

among data brokers and products.[113] Competition in the data industry pushes brokers to improve accuracy, but errors nonetheless persist due to data gap-filling and downstream aggregation.[114] It is like the child's game of "telephone" in which the first child whispers a secret in the ear of the nearest player and the players seek to repeat the secret ear-to-ear until the last player must reveal what she heard—which has usually changed significantly by the time it has reached the last child's ears.[115]

Furthermore, the lack of transparency and inability to contest collected data and related assumptions are concerning. Consumers may be upset to learn that a company offers them different deals and levels of care based on predictive scores. Neustar, for example, instantly scores consumers when they call a client company's customer service center to alert agents what to offer that caller.[116] As another example, Wayfair.com may offer consumers different deals based on whether its algorithms classify the consumers as "hunters" or "gatherers" when searching this online-sellers' website.[117]

Consumer scoring is rampant and increasingly nuanced as individuals become subject to dozens or hundreds of secret consumer scores.[118] The following are among the long list of scores highlighted by a recent report of the World Privacy Forum (WPF—a non-profit public interest research and consumer education group):

- Experian's ChoiceScore for financial risk;
- Experian's Median Equivalency Score for seriously derogatory behavior;

---

113. RAMIREZ ET AL., *supra* note 1, at 36-38.

114. *Id.*

115. This was a common party game when I was a child (long before video games and iPads!). It was always surprising how the secret changed when whispered from ear-to-ear despite each child's earnest attempt to simply repeat the secret. Gossip is very similar in the sense that information changes the further it gets from the original source.

116. *Neustar PlatformOne*, NEUSTAR, http://www.neustar.biz/marketing-solutions (last visited Jan. 7, 2015).

117. Abram Brown, *How Wayfair Sells Nearly $1 Billion Worth of Sofas, Patio Chairs and Cat Playgrounds*, FORBES (Apr. 16, 2014, 6:00 AM), http://www.forbes.com/sites/abrambrown/2014/04/16/how-wayfair-sells-nearly-1-billion-worth-of-sofas-patio-chairs-and-cat-playgrounds/print/ (emphasizing how the company has flourished using its algorithms and tracking consumers' buying habits). "Hunters" are customers who indicate a propensity to search for and buy a particular item after price comparisons; such customers receive special deals as a means to capture their business while "gatherers," who indicate a willingness to "window-shop," do not receive these deals. *Id.*

118. *See generally* DIXON & GELLMAN, *supra* note 7.

- Consumer Profitability Score to target profitable households;
- Job Security Score;
- Acxiom's Consumer Prominence Indicator Score for a consumer's market activity;
- Equifax's Discretionary Spending Index Score;
- Experian's Veriscore for customer value potential;
- Churn Score to predict when a customer will move business to another merchant;
- Target's Pregnancy Predictor Score;
- Klout Score using social media to track one's number of Followers;
- Employment Success Score predicting job success using Facebook data;
- Casino Gaming Propensity Score;
- Economic Stability Indicator.[119]

The WPF report also explains how some of these scores go beyond assessments based on an individual's financial information to include consideration of that individual's connections, networks, and "friends" on social media.[120] Advertisers may reach out to a highly valued customer's "friends" on Facebook to market goods and services presuming that the consumer's friends will share characteristics they deem valuable for their business.[121] However, a company also may downgrade a consumer's value based on "friends" and connections deemed less worthy in the company's valuation.[122] "Social credit" also considers consumers' influence on social media more generally, including followers on Twitter and friends on Facebook.[123] Consumers may even be judged based on the music they listen to on Spotify and Pandora.

The FTC also released a 2014 report describing how data brokers use complex models and algorithms to segment and score

119. *Id.* at 42-79 (discussing all the different types of scores and including scoring well beyond what is noted here).

120. *Id.* at 72-76.

121. *See* Cullerton, *supra* note 19, at 814-17 (discussing valuations based on social media connections).

122. *See id.* at 816.

123. *Id.* at 816-17.

consumers.[124] The FTC based its report on information the Commission gathered from nine of the largest data brokers in the United States.[125] These brokers covered a cross section of the industry ranging from those that focus on products for marketing to those specializing in risk mitigation and people searches.[126] Specifically, the FTC gathered details about the following: "The nature and sources of consumer information [the data brokers] collect. How the companies use, maintain, and distribute that information. If they allow consumers to see the information they collect, if consumers can correct inaccuracies or opt out of having their information sold."[127] In conducting its study, the FTC voiced its concerns for data privacy while also acknowledging how data collection and sharing benefit consumers and the economy by helping address fraud and allowing companies to better market their goods and services.[128]

---

124. RAMIREZ ET AL., *supra* note 1, at 19-39 (discussing these marketing products and the many categorizations companies use in determining consumer offers and treatment). The FTC gathered information by sending out Model Orders requiring the selected data brokers to produce information regarding the companies' products and services, general data collection practice, complaint and inquiry record, policies regarding consumer access to the collected data, and a list of the company's largest consumers. *Id.* at app. A. The orders also asked the brokers to provide a Special Report detailing a variety of information, including the nature and purpose of products and services that use personal data, methods of accuracy evaluation, transparency, consumer access to collected data, and consumers' ability to correct or delete information collected. *Id.*

125. Janna Herron, *FTC Takes on Data Brokers*, BANKRATE (Dec. 19, 2012, 4:00 PM), https://web.archive.org/web/20131003065653/http://www.bankrate.com/financing/credit-cards/ftc-takes-on-data-brokers/; *see* RAMIREZ ET AL., *supra* note 1, at 9-10.

126. *See* RAMIREZ ET AL, *supra* note 1, at i.

127. *Id.*; *see FTC to Study Data Broker Industry's Collection and Use of Consumer Data*, FED. TRADE COMMISSION (Dec. 18, 2012), http://www.ftc.gov/news-events/press-releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data; *see also, e.g.*, Letter from Maneesha Mithal, Assoc. Dir., Fed. Trade Comm'n Div. of Privacy & Identity Prot., to 4Nannies 2 (May 2, 2013), *available at* http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-warns-data-broker-operations-possible-privacy-violations/130507databrokers4nanniesletter.pdf ("At this time, we have not evaluated your company's practices to determine whether they comply with the FCRA. However, we encourage you to review your products and services, as well as your policies, employee-training, and other procedures for compliance.").

128. *FTC to Study Data Broker Industry's Collection and Use of Consumer Data*, *supra* note 127.

In May 2014, the FTC issued its report based on the information collected.[129] It highlighted some benign classifications such as "Consumers Interested in Buying Camping Gear," but also revealed questionable segments based on combinations of age, ethnicity, and/or income such as: "Urban Scramble" and "Mobile Mixers" ("high concentration of Latino and African-American consumers with low incomes"), "Thrifty Elders" (singles in late 60s/early 70s with low income), "Work & Causes" (lower-income consumers in late 40s/early 50s in multi-unit dwellings), "Timeless Traditions" (immigrants, many of retirement age with limited English and lower incomes), "Downtown Dwellers" (lower-income singles in metro areas with limited education and working clerical or service jobs to "make[] ends meet"), and "Metro Parents" (single parents with limited education, living "urban life on a small budget").[130] Classifications also may take into account health conditions such as diabetes and high cholesterol, only to name a few.[131]

The FTC also found that five of the nine brokers it studied provide analytic products "based on algorithms that consider hundreds or thousands of data elements," and may be converted into a variety of scores for consumers.[132] Scores may assess consumers' likely response or purchase rates, influence and presence on the Internet, and purchasing power more generally.[133] For example, companies use "social influence scores to ensure that they advertise their products to these particular consumers, with the expectation that these consumers will, in turn, tout these products to their friends and followers."[134]

Such scoring and "social influence" assessments raise serious relational concerns by judging individuals based on their connections and essentially who they "hang out with" on social media.[135] Furthermore, consumer scoring more generally has raised red flags for many government regulators and consumer advocates. Professor Frank Pasquale has studied the broker industry and highlighted how

129. RAMIREZ ET AL., *supra* note 1, at i-ii.
130. *Id.* at 19-21 (internal quotation marks omitted) (also listing more segments).
131. *Id.* at 47.
132. *Id.* at 31.
133. *Id.* at iii.
134. *Id.* at 31.
135. Cullerton, *supra* note 19, at 825-26.

these consumer scores perpetuate discriminatory contracting.[136] He stated with respect to e-scores "'I'm troubled by the idea that some people will essentially be seeing ads for subprime loans, vocational schools and payday loans . . . while others might be seeing ads for regular banks and colleges, and not know why.'"[137]

Mierzwinksi and Chester also have questioned whether these scores cross over the line from valid marketing or permissible data collection to credit reporting and assessment governed by the FCRA.[138] Currently, the FCRA does not generally apply to broader consumer scores or ratings because it only applies to credit scores or reports used for credit, employment, or insurance determinations.[139] Similarly, consumer scores usually fall outside the Equal Credit Opportunity Act (ECOA), which bars consideration of factors like race, gender, and marital status in extending credit.[140] Those creating consumer scores also are generally not obligated to follow Fair Information Practices or provide due process to consumers.[141] Concerns regarding this lack of regulation and transparency have spurred the FTC and the CFPB to study related issues.[142]

II. LEGAL RESTRICTIONS ON DATA BROKERS AND CREDIT SCORING

The law governing privacy and the data broker industry is far from clear. As the GAO has stated, "In relation to data used for marketing purposes, no federal statute provides consumers the right to learn what information is held about them and who holds it."[143] This Section therefore aims only to provide a brief sketch of the key regulations and potential restrictions on data brokers' use of consumer information to create scores or valuations. Namely, the FTC regulates data privacy, and its chief enforcement tool is the FCRA governing credit reporting that impacts consumers' access to

136. Singer, *supra* note 9.
137. *Id.* (quoting Frank Pasquale).
138. Mierzwinski & Chester, *supra* note 12, at 861-62.
139. DIXON & GELLMAN, *supra* note 7, at 44.
140. *Id.* at 9-10.
141. *Id.* at 10 (summarizing problems associated with consumer scoring).
142. Mierzwinski & Chester, *supra* note 12, at 878-81 (calling for these agencies to study these issues and establish clear policy in light of the growing digital marketplace).
143. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-663, INFORMATION RESELLERS: CONSUMER PRIVACY FRAMEWORK NEEDS TO REFLECT CHANGES IN TECHNOLOGY AND THE MARKETPLACE 16 (2013).

credit, insurance, and employment.[144] Nonetheless, this Act generally does not govern broad-based consumer scoring and ratings companies use for marketing and other consumer interactions.[145] This leaves the area ripe for regulation by the FTC and/or CFPB.

A. FTC and the FCRA

The FCRA generally governs consumer reports and imposes duties upon consumer reporting agencies.[146] The Act requires these agencies to provide consumers with all information in their credit files upon request, including information about payment histories and the identities of all those who received the reports.[147] Consumers have a right to one free copy of their report from each reporting agency per year.[148] They also may have a right to more than one free copy per year in some states.[149] Furthermore, consumers may obtain a free copy of their credit file in various circumstances such as identity theft or when "[a] person has taken adverse action against you because of information in your credit file."[150] Upon consumer request, reporting agencies also must provide consumers with "[t]he dates, original payees, and amounts of any checks [written by the consumers] upon which [the agency] based any adverse characterization of the consumer[s]" in their reports.[151]

In addition, reporting agencies must supplement reports with a statement setting forth consumers' FCRA rights.[152] This statement notifies consumers that the reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information generally within thirty days after one notifies the agency of the discrepancy.[153] Consumers bear the burden, however, to do their due diligence in obtaining their credit reports, checking them for accuracy, and notifying the agency reporting the inaccurate information in writing

144. Fair Credit Reporting Act, 15 U.S.C. § 1681(a) (2012).
145. Mierzwinski & Chester, *supra* note 12, at 860.
146. 15 U.S.C. § 1681(a)-(b).
147. *Id.* § 1681g(a).
148. *Id.* § 1681j(a)(1)(A).
149. *See* A SUMMARY OF YOUR RIGHTS UNDER THE FAIR CREDIT REPORTING ACT, *available at* http://www.cheyney.edu/human-resources/documents/1-1-2013Summary_of_Rights.pdf (last visited Jan. 7, 2015).
150. *Id.*
151. 15 U.S.C. § 1681g(a)(4).
152. 16 C.F.R. § 601.1(b) (2001).
153. *Id.* § 601 app. A.

of any discrepancies.[154] The FCRA does not require agencies to give consumers their scores free of charge, but they must disclose all the information in credit files.[155] Furthermore, agencies have no duty to remove accurate information unless it is more than seven years old, or ten years old in the case of bankruptcies.[156]

Notably, these rules only apply to consumer reports as defined by the FCRA.[157] Section 1681a(d)(1) of the FCRA defines a consumer report as:

> [A]ny written, oral, or other communication of any information 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 which is used or expected to be used or collected in whole or in part for the purpose of serving 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 section 1681b of this title.[158]

Under this definition, the FCRA generally applies to the traditional credit reports that most consumers have heard of or seen from companies like Experian, TransUnion, and Equifax.[159] It also applies to reports created by lesser-known reporting agencies.[160] One such powerful agency that remains largely unknown is Advanced Resolution Services, Inc., which is a subsidiary of Visa, Inc. that assists in evaluating risks related to credit cardholders' accounts.[161]

---

154. One may go online to www.ftc.gov to obtain information on getting their annual free credit reports (one from each of the three main agencies—Experian, Equifax, and Transunion). *Get My Free Credit Report*, FED. TRADE COMMISSION, http://www.ftc.gov/faq/consumer-protection/get-my-free-credit-report (last visited Jan. 7, 2015). Consumers also may call 1-877-FTC-HELP to file a complaint or to obtain free information about consumer issues. *About Us*, FED. TRADE COMMISSION, http://www.consumer.ftc.gov/about-us (last visited Jan. 7, 2015).

155. 15 U.S.C. § 1681j(f)(1).

156. Fair Credit Reporting Act, Pub. L. No. 91-508, § 605(a), 84 Stat. 1128, 1129-30 (1970) (codified as amended at 15 U.S.C. § 1681c(a)).

157. 15 U.S.C. § 1681a(d).

158. *Id.* § 1681a(d)(1).

159. Mierzwinski & Chester, *supra* note 12, at 846.

160. *See* 15 U.S.C. § 1681a(f).

161. *See Company Overview of Advanced Resolution Services, Inc.*, BLOOMBERG BUSINESSWEEK, http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=108558215 (last visited Jan. 7, 2015). There is not a great deal of information on ARS available on the Internet or elsewhere. I learned

The FCRA generally does not apply to internal credit determinations that a company may make based on data it has collected from its own tracking or from parties other than credit reporting agencies.[162] The Act also does not apply to data brokers who compile information for marketing purposes or to determine general consumer treatment.[163] These companies postulate that their data collection is outside the purview of the FCRA because they do not necessarily collect data or issue scores in connection with lending, insurance, or employment decisions.[164] Nonetheless, these companies collect information about consumers' "credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, [and] mode of living."[165]

That said, the FTC has been investigating privacy issues and data collection in broader contexts beyond traditional credit reporting. The FTC has authority to regulate data privacy and is appropriately concerned with the expansion of data collection.[166] Section 45 of the Federal Trade Commission Act (FTC Act) prohibits "unfair or deceptive acts or practices in or affecting commerce."[167] The FTC therefore aims to increase transparency in the marketplace in order to protect consumers from deception.[168] It also targets deceptive practices that place consumers' privacy at risk with respect to not only financial information under the FCRA, but also to health information and data regarding children.[169]

---

about ARS when it sent me notice of suspected fraudulent use of my credit card. After providing proof of identity, ARS sent me their "Consumer Report" on me along with statements alerting me of my rights. Letters from ARS to author (letters on file with author).

162. *See* Mierzwinski & Chester, *supra* note 12, at 846.

163. *See id.* at 860.

164. *See id.* at 858-60.

165. 15 U.S.C. § 1681a(d)(1).

166. *See* Mierzwinski & Chester, *supra* note 12, at 877.

167. Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (2012).

168. *Id.* § 45(a)(2); *see also* Mierzwinski & Chester, *supra* note 12, at 876-77.

169. Gramm–Leach–Bliley Act, Pub. L. No. 106-102, §§ 131-33, 113 Stat. 1338, 1382-83 (1999) (codified in scattered sections of 12 and 15 U.S.C.); Children's Online Privacy Protection Act of 1998, Pub. L. 105-277, § 1306, 112 Stat. 2681-728, 2681-734 (codified as amended at 15 U.S.C. § 6505); Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.); Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226 (2009) (codified in scattered sections of 42 U.S.C.).

> [T]he FTC conducts its investigations with a focus on reasonableness—a company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities.[170]

In this vein, the FTC has been investigating online privacy issues and dangers associated with companies' collection and use of consumers' data generally without knowledge or approval.[171] In March 2012, the FTC issued a report setting forth best practices for companies to follow in order to better protect consumers' privacy and give them greater control over the collection and use of their personal data.[172] The lengthy report shed light on companies' collection of consumers' information from not only direct interaction, but also public records and information purchased from other companies without consumers' consent.[173] The FTC noted that most consumers do not realize which companies have their data or what information the companies have, and it is very difficult for consumers to access and to verify collected data, even when data brokers offer that option.[174] It is tough for even the savviest consumers to investigate the winding and uncertain trails of data sources.[175]

The FTC report concluded that there is a lack of laws requiring data brokers to maintain the privacy of consumer data that falls outside of the FCRA's scope.[176] It therefore recommended that Congress consider enacting legislation requiring all data brokers to protect privacy and ensure data security and breach notification for

---

170. *Protecting Consumer Information: Can Data Breaches Be Prevented?: Hearing Before the Subcomm. on Commerce, Mfg., and Trade of the H. Comm. on Energy & Commerce*, 113th Cong. 4 (2014) (statement of Edith Ramirez, Chairwoman of the Federal Trade Commission).

171. *FTC Issues Final Commission Report on Protecting Consumer Privacy: Agency Calls on Companies to Adopt Best Privacy Practices*, FED. TRADE COMMISSION (Mar. 26, 2012) http://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy.

172. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

173. *Id.* at 26, 68-69.

174. *Id.* at 68-69.

175. *Id.* at 5-43.

176. *Id.* at 68-70.

consumers.[177] The FTC emphasized that brokers should disclose details about their data collection and use of consumers' information, provide access to collected data, and give consumers choice regarding data practices that are inconsistent with the context of a particular transaction or the business relationship with the consumer.[178] The FTC further suggested that data brokers should establish a centralized website where consumers could get information about brokers' practices and consumer options for controlling data use.[179] The Commission nonetheless commended the progress that had been made regarding Do Not Track, although its use is limited.[180]

In the summer of 2012, the FTC also pursued enforcement actions regarding data privacy. For example, the FTC fined Spokeo $800,000 for marketing a service that provides consumer reports and background checks.[181] This was the first time the FTC initiated an enforcement action related to "the sale of Internet and social media data in the employment screening context."[182] According to the FTC, Spokeo gathered consumers' personal information from hundreds of online and offline data sources to create and sell consumer profiles that included information such as name, address, age range, email addresses, "hobbies, ethnicity, religion, participation on social networking sites, and photos."[183] Spokeo nonetheless was not protecting the information or taking steps to assure its accuracy as required under the FCRA.[184] This amounted to unfair and deceptive acts in commerce.[185]

In spring of 2013, the FTC issued orders to ten companies after conducting a test-shopper operation that indicated that these

177. *Id.* at 1-37 (but concluding that such legislation should not apply to companies that collect only non-sensitive data from fewer than 5,000 consumers a year).

178. *Id.* at 22-70. The report is very lengthy and contains a broad range of principles for protecting consumers' privacy and access to data collected about them. *Id.*

179. *Id.* at 69.

180. *Id.* at 52-53. The FTC also is working with the Department of Commerce and stakeholders to develop industry-specific codes of conduct. *Id.* at 73.

181. *Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA*, *supra* note 80.

182. *Id.*

183. *Id.*

184. *Id.*

185. *Id.*

companies might be violating the FCRA.[186] As "part of a worldwide privacy protection effort," FTC test-shoppers posed as parties seeking consumer information to make insurance, credit, or employment decisions.[187] The letters were not official notice by the Commission that any of the named companies violated the FCRA, but they alerted companies to evaluate their practices to determine whether they are consumer reporting agencies, and if so, to comply with that law.[188]

The FTC conducted this operation in conjunction with Global Privacy Enforcement Network, which "connects privacy enforcement authorities to promote and support cooperation in cross-border enforcement of laws protecting privacy."[189] Specifically, the ten companies flagged for potential violations included:

> Two companies that appeared to offer "pre-screened" lists of consumers for use in making firm offers of credit: ConsumerBase and ResponseMakers;
>
> Two companies that appeared to offer consumer information for use in making insurance decisions: Brokers Data and US Data Corporation; and
>
> Six companies that appeared to offer consumer information for employment purposes: Crimcheck.com, 4Nannies, U.S. Information Search, People Search Now, Case Breakers, and USA People Search.[190]

These companies raised red flags by indicating willingness to sell consumer information without abiding by FCRA requirements such as verifying that the potential purchasers of the information planned to use the data for legitimate purposes.[191]

Since that time, the FTC has brought more enforcement actions against privacy violators.[192] For example, the FTC obtained $3.5 million, the second-largest penalty in a FCRA matter, against

---

186. *FTC Warns Data Broker Operations of Possible Privacy Violations*, FED. TRADE COMMISSION (May 7, 2013), http://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations.

187. *Id.*

188. *See* Letter from Maneesha Mithal to 4Nannies, *supra* note 127, at 1.

189. *See FTC Warns Data Broker Operations of Possible Privacy Violations*, *supra* note 186.

190. *Id.*

191. Fair Credit Reporting Act, 15 U.S.C. § 1681e(e)(2) (2012).

192. *See, e.g.*, HTC America, Inc., No. C-4406, FTC File No. 122-3049 (June 25, 2013); Facebook, Inc., No. C-4365, FTC File No. 092-3184 (July 27, 2012); Google, Inc., No. C-4336, FTC File No. 102-3136 (Oct. 13, 2011); Twitter, Inc., No. C-4316, FTC File No. 092-3093 (Mar. 2, 2011).

Certegy Check Services in August 2013.[193] Certegy is one of the nation's largest check-cashing-authorization services that compiles people's personal information and uses it to help retailers decide whether to accept a customer's personal check.[194] The company allegedly failed to follow proper dispute procedures.[195] It also failed to institute reasonable procedures for assuring the accuracy of information provided to its merchant clients, which included grocery stores and other common places where consumers would often suffer great detriment from having their checks denied.[196] The FTC settled a factually similar lawsuit against TeleCheck for $3.5 million in January 2014.[197]

The FTC and its Commissioner have continued to voice significant concerns regarding Big Data. Commissioner Julie Brill stated in her address, *Big Data and Consumer Privacy: Identifying Challenges, Finding Solutions*, at the Woodrow Wilson School of Public and International Affairs at Princeton University on February 20, 2014:

> As we further examine the privacy implications of big data analytics, I believe one of the most troubling practices that we need to address is the collection and use of data—whether generated online or offline—to make sensitive predictions about consumers, such as those involving their sexual orientation, health conditions, financial condition, and race.[198]

Commissioner Brill went further to highlight companies' discriminatory use of data to segment consumers deemed risky or lower value,[199] making them vulnerable to targeted offers for payday and other high-cost fringe lending products.[200]

---

193. *Certegy Check Services to Pay $3.5 Million for Alleged Violations of the Fair Credit Reporting Act and Furnisher Rule*, FED. TRADE COMMISSION (Aug. 15, 2013) http://www.ftc.gov/news-events/press-releases/2013/08/certegy-check-services-pay-35-million-alleged-violations-fair.

194. *Id.*

195. *Id.*

196. *Id.*

197. *TeleCheck to Pay $3.5 Million for Fair Credit Reporting Act Violations*, FED. TRADE COMMISSION (Jan. 16, 2014), http://www.ftc.gov/news-events/press-releases/2014/01/telecheck-pay-35-million-fair-credit-reporting-act-violations.

198. Julie Brill, Comm'r, Fed. Trade Comm'n, Big Data and Consumer Privacy: Identifying Challenges, Finding Solutions, Address at the Woodrow Wilson School of Public and International Affairs at Princeton University 3 (Feb. 20, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/202151/140220princetonbigdata_0.pdf.

199. *See id.* at 3-5 (noting alarming facts regarding categorizations).

200. *See generally* Amy J. Schmitz, *Females on the Fringe: Considering Gender in Payday Lending Policy*, 89 CHI.-KENT L. REV. 65 (2013).

Accordingly, the FTC's statements and recent enforcement actions have been influential in shaping companies' data privacy and security practices.[201] This essentially has developed a "common law" for data practices.[202] FTC actions and settlements have a ripple effect, as they provide standards and best practices for brokers to follow and arouse companies' fear that they will face expensive audits if they breach these standards.[203]

Furthermore, the FTC has an opportunity to play a special role in protecting the consumer "have-nots." It may use its powers to curb unfair practices that seek to take advantage of vulnerable consumers.[204] It has become clear that data privacy abuses and improprieties persist, and there is need for legislation or expanded regulations to curb data brokers' improper practices that evade the FCRA. Furthermore, the FTC should work in tandem with the CFPB in regulating data privacy with respect to financial products and services.

B. CFPB

The CFPB created under Dodd–Frank has the power to restrict "unfair, deceptive, or abusive acts" that are "likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers" where this injury "is not outweighed by countervailing benefits to consumers or to competition."[205] Dodd–Frank defines "abusive" to include contextual consideration of race,

---

201. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM L. REV. 583, 585 (2014).

202. *See generally id.* (arguing that the FTC's enforcement actions and settlements have created a "common law" for privacy regulation, but urging the FTC to be bolder in its actions).

203. *Id.* at 600-56; Daniel J. Solove & Woodrow Hartzog, *The FTC and Privacy and Security Duties for the Cloud*, 13 Privacy & Security L. Rep. (BNA) No. 577, at 1-4 (Apr. 7, 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2424998 (discussing the influences of FTC actions on data practices and cases indicating that companies may be held responsible for hiring data service providers that do not follow proper privacy and security standards).

204. Solove & Hartzog, *supra* note 203, at 3-4.

205. Dodd–Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 1031, 124 Stat. 1376, 2005-06 (2010) (codified at 12 U.S.C. § 5531 (2012)). Dodd–Frank includes payday lending within its references to small-dollar lending, and has expressed its concern with payday lending. CONSUMER FIN. PROT. BUREAU, PAYDAY LOANS AND DEPOSIT ADVANCE PRODUCTS: A WHITE PAPER OF INITIAL DATA FINDINGS 1, 4 (2013), *available at* http://files.consumerfinance.gov/f/201304_cfpb_payday-dap-whitepaper.pdf.

gender, and other such classifications.[206] Dodd–Frank also directs the CFPB to research "'access to fair and affordable credit for traditionally underserved communities'" as well as effective disclosures to address consumer propensities.[207] This has opened the door to the CFPB's possible action in the area of consumer reporting and scoring.

Dodd–Frank also allows for double-barrel federal/state regulation. The Act mandates that the CFPB must coordinate with states in regulating financial products and services, and preserve states' power to provide greater protections than those federal law provides.[208] This furthers federalism by preserving states' power to enforce their own consumer protection laws for the benefit of their citizens.[209] Dodd–Frank also empowers state attorneys general to enforce the Act's prohibitions and any rules the CFPB promulgates.[210] A broad reading of Dodd–Frank also gives state attorneys general the power to investigate potential federal violations.[211]

Although the FTC has remained at the helm in regulating credit reporting, the CFPB also has been looking at how its regulations could extend to consumer reporting on broader levels.[212] The CFPB may exercise its supervisory power "by requiring the submission of reports and conducting examinations to: (1) Assess compliance with Federal consumer financial law; (2) obtain information about such persons' activities and compliance systems or procedures; and (3) detect and assess risks to consumers and to consumer financial markets."[213] The CFPB may therefore review the processes used by credit reporting companies in compiling their reports and ensure that companies comply with requirements of the FCRA.[214] Nonetheless, "because the rule itself does not require any entity to alter its

206. *See* Mark Totten, *Credit Reform and the States: The Vital Role of Attorneys General After Dodd–Frank*, 99 IOWA L. REV. 115, 132-54 (2013) (noting the ambiguity, but proposing broad reading of the Act).

207. Jim Hawkins, *The Federal Government in the Fringe Economy*, 15 CHAP. L. REV. 23, 36-38 (2011) (quoting § 1013(b)(1)(B), 124 Stat. at 1968).

208. *See* § 1015, 124 Stat. at 1974; *see also* Hawkins, *supra* note 207, at 55.

209. Hawkins, *supra* note 207, at 54-56.

210. Totten, *supra* note 206, at 126-34.

211. *See id.* at 132-54 (noting the ambiguity, but proposing broad reading of the Act).

212. *See* Defining Larger Participants of the Consumer Reporting Market, 77 Fed. Reg. 42,874 (July 20, 2012) (to be codified at 12 C.F.R pt. 1090).

213. *Id.*

214. *Id.*

provision of consumer reporting products or services, any estimate of the amount of increased compliance would be a prediction of market participants' behavior."[215]

Still, the CFPB's power may extend to data brokers and consumer scoring beyond traditional credit reporting.[216] In 2012, the CFPB promulgated a final rule on "Defining Larger Participants of the Consumer Reporting Market."[217] It promulgated this rule in order to facilitate "the supervision of nonbank covered persons active in that market" for consumer reporting.[218] It thus focused its definition to covered persons with annual receipts derived from the business of consumer reporting in excess of $7 million.[219] It also broadly construed "'consumer reporting'" as "'collecting, analyzing, maintaining, or providing consumer report information or other account information . . . used or expected to be used in connection with any decision [by another person] regarding the offering or provision of a consumer financial product or service.'"[220]

However, the CFPB's coverage includes large exceptions. It does not include the collection of data that relates to a company's own transactions or experiences with consumers.[221] The CFPB's coverage also excludes transactions between a consumer and an affiliate to another person engaged in consumer reporting; "approval of a specific extension of credit"; employment decisions; government licenses; and residential leases.[222] These exceptions, along with the $7 million threshold, significantly narrow the CFPB's regulatory scope.

---

215. *Id.* at 42,892.

216. *Id.* at 42,898.

217. *See id.* at 42,874. The authority to "supervise" nonbank larger participants of the consumer reporting market is derived from 12 U.S.C. § 5514. Marc S. Roth & Charles Washburn, *Data Brokers Face Blurring Lines, Increased Regulatory Risks*, BLOOMBERG BNA (Aug. 22, 2012), http://about.bloomberglaw.com/practitioner-contributions/data-brokers-face-blurring-lines/.

218. Defining Larger Participants of the Consumer Reporting Market, 77 Fed. Reg. at 42,874. The final rule explicitly notes that "[i]t does *not* impose new substantive consumer protection requirements. Nor does it delineate the scope for the Fair Credit Reporting Act (FCRA), provisions of the Dodd-Frank Act related to consumer reporting activities, or any other Federal consumer financial law." *Id.* (emphasis added).

219. *Id.* at 42,874, 42,876.

220. *Id.* at 42,884 (quoting 12 U.S.C. § 5481(15)(A)(ix) (2012)).

221. *Id.* at 42,885.

222. *Id.* at 42,885-87.

Nonetheless, some data brokers that provide consumer scores are under the CFPB's jurisdiction in regulating "larger participants" in the "consumer reporting" area, thus opening the door to CFPB study of consumer scoring.[223] Furthermore, the CFPB has authority to issue regulations and take enforcement actions with respect to the Gramm–Leach–Bliley Act's prohibition on financial institutions from sharing nonpublic, personally identifiable customer information with nonaffiliated third parties without giving customers an opportunity to opt out.[224] The CFPB's enforcement authority generally is primarily over nondepository institutions and depository institutions with over $10 billion in assets.[225] Moreover, the FTC remains active in policing the data broker industry and pursuing legislative reforms targeting consumer scoring.[226]

C. Federal Discrimination Law

Outright discrimination offends public values as well as the United States Constitution. Constitutional equal protection law precludes state laws that discriminate against women, minorities, and other suspect classifications.[227] With respect to financial transactions,

223. Based on the description of these e-scores in the *New York Times* article, see Natasha Singer, *Secret E-Scores Chart Consumers' Buying Power*, N.Y. TIMES (Aug. 18, 2012), http://www.nytimes.com/2012/08/19/business/electronic-scores-rank-consumers-by-potential-value.html?pagewanted=all&_r=0, it appears that these scores are calculated and provided to other parties to be used "'regarding the offering or provision of [particular] consumer financial product[s] or service[s].'" Defining Larger Participants of the Consumer Reporting Market, 77 Fed. Reg. at 42,884 (quoting 12 U.S.C. § 5481(15)(A)(ix)); *see also id.* at 42,874 n.8 (defining consumer reporting for the purposes of defining larger participants in the consumer reporting market); Roth & Washburn, *supra* note 217 (explaining that "[o]nly data brokers with more than $7 million in annual receipts resulting from relevant consumer reporting activities would be subject to CFPB supervision").

224. M. MAUREEN MURPHY, CONG. RESEARCH SERV., RS20185, PRIVACY PROTECTION FOR CUSTOMER FINANCIAL INFORMATION 2-3 (2014).

225. *Id.* at 5. The CFPB's rules still may apply to smaller depository institutions. *Id.*

226. Roth & Washburn, *supra* note 217.

227. John A. Ward III, Note, *Husband and Wife—Contracts—Married Woman Not Liable on Mercantile or Trading Contract Unless Disability of Coverture Removed*—Wyner v. Express Publishing Co.*, 288 S.W.2d 583 (Tex. Civ. App.—San Antonio 1956, error ref'd n.r.e.)*, 34 TEX. L. REV. 1094, 1094-96 (1956) (highlighting courts' applications of covertures statutes directing that a married woman cannot enter binding contracts). It was not until 1981, however, that the U.S. Supreme Court finally held that laws allowing a husband to sell or encumber marital

the Equal Credit Opportunity Act (ECOA) prohibits creditors from discriminating against an applicant "with respect to any aspect of a credit transaction" on the basis of race, sex, marital status, religion, or national origin.[228] The ECOA thus precludes lenders from offering substantially different interest rates or pricing structures to those in protected groups, and from targeting or discouraging applications from protected groups.[229] Specifically, lenders may not evaluate applications on a prohibited basis or discriminate against applicants because their income comes from a part-time job, alimony, child support, veterans' assistance, or other public assistance.[230] Lenders must also notify applicants of adverse actions taken in connection with an application for credit in an accurate and timely manner.[231]

Nonetheless, the ECOA has been criticized as largely ineffective in addressing the subtle discrimination that occurs with respect to lending and credit scoring.[232] The Act essentially addresses only blatant disparate treatment or the rare disparate impact cases that are sufficiently well documented.[233] For example, a plaintiff may survive a motion to dismiss where she proves disparate treatment based on evidence that a creditor used gender-based epithets in threatening to increase the amount owed on a debt.[234] The Act also may stop a credit-reporting agency from blatantly downgrading consumers based on race.[235] However, even disparate treatment

---

property without a wife's consent were unconstitutional. *See* Kirchberg v. Feenstra, 450 U.S. 455, 456 (1981).

228. 15 U.S.C. § 1691(a)(1) (2012).

229. ALYS COHEN ET AL., CREDIT DISCRIMINATION 22-23, 25 (Nat'l Consumer Law Ctr., 5th ed. 2009).

230. *Id.* at 54-55, 144.

231. *Id.* at 129, 148, 187, 196, 198 (noting that creditors also may not consider likelihood to have children).

232. *See* Melissa B. Jacoby, *The Debt Financing of Parenthood*, 72 LAW & CONTEMP. PROBS. 147, 173 n.153 (2009) (noting that "'lenders continue to deny loans to creditworthy consumers and practice gender and spousal discrimination'" despite passage of the ECOA (quoting Willy E. Rice, *Race, Gender, "Redlining," and the Discriminatory Access to Loans, Credit, and Insurance: An Historical and Empirical Analysis of Consumers Who Sued Lenders and Insurers in Federal and State Courts, 1950-1995*, 33 SAN DIEGO L. REV. 583, 585-86 (1996))).

233. *See* DIXON & GELLMAN, *supra* note 7, at 10, 13-14.

234. Sharp v. Chartwell Fin. Servs. Ltd., No. 99-C-3828, 2000 WL 283095, at *1, *3-5 (N.D. Ill. Mar. 6, 2000) (finding plaintiffs survived the creditor's motion to dismiss on their ECOA and FDCPA claims where they had specific evidence of harassing threats with gender-based and racial epithets).

235. *See* DIXON & GELLMAN, *supra* note 7, at 10.

claimants face difficulties in finding and obtaining company memos or other evidence to prove their allegations.[236]

Disparate impact cases are particularly difficult to prove. Claimants bear a tough burden in (1) establishing that the defendant employed a specific policy or practice in order to discriminate and (2) demonstrating with statistical data that the policy or practice had a demonstrable adverse effect on the claimants.[237] Furthermore, in lending and other consumer contract cases, defendants may easily hide misuse of biases or stereotypes in determining rates and prices under the guise of "business justifications."[238] "Discretionary pricing" is so common and accepted in economic and marketing

236. *See* COHEN, *supra* note 229, at 69-71. In addition, women may be able to use the FDCPA to recover against debt collectors who harass them with threats against their children or negative comments about their marriages and capacity to raise children. *See* Bingham v. Collection Bureau, Inc., 505 F. Supp. 864, 866, 868-69, 874-76 (D.N.D. 1981) (awarding plaintiff damages under the FDCPA where a collector told her that she "shouldn't have children" due to her hospital debt); Fed. Trade Comm'n v. Check Investors, Inc., 502 F.3d 159, 162-63 (3d Cir. 2007) (affirming injunction and fines against a company that told female debtors that their children would see them "'being taken away in handcuffs,'" and "'be bringing their mommy care packages in prison'"); Black v. Aegis Consumer Funding Grp., Inc., No. CIV. A. 99-0412-P-S, 2001 WL 228062, at *2-9 (S.D. Ala. Feb. 8, 2001) (awarding damages under the FDCPA where the collectors told a mother that they would take her "'kids' clothing,'" and hounded her about whether her marriage was the reason she was not paying her debts).

237. *See* Susan D. Carle, *A Social Movement History of Title VII Disparate Impact Analysis*, 63 FLA. L. REV. 251, 257, 297-98 (2011) (stating that it is "very rare for plaintiffs [in disparate impact cases] other than highly sophisticated and well-funded litigants, such as the U.S. Department of Justice, to prevail under Title VII" in the employment context).

238. Masudi v. Ford Motor Credit Co., No. 07-CV-1082, 2008 WL 2944643, at *5 (E.D.N.Y. July 31, 2008) (dismissing an ECOA claim for failure to meet this burden of proof, and dismissing the FDCPA claim because the defendant was a creditor and not a collector). Borrowers also have launched "reverse redlining" cases against lenders that target racial minority communities for overpriced loans, but these actions are difficult for plaintiffs and their attorneys to recognize, let alone prove and bring to successful fruition. *See generally* Andrew Lichtenstein, *United We Stand, Disparate We Fall: Putting Individual Victims of Reverse Redlining in Touch with Their Class*, 43 LOY. L.A. L. REV. 1339 (2010) (discussing reverse redlining claims); Pouya Bavafa, *The Intentional Targeting Test: A Necessary Alternative to the Disparate Treatment and Disparate Impact Analyses in Property Rentals Discrimination*, 43 COLUM. J.L. & SOC. PROBS. 491, 496 (2010) (discussing reverse redlining in housing rentals and "substantial difficulty establishing discrimination under traditional civil rights jurisprudence").

circles that consumers are bound to fail in any attempts to show its discriminatory underpinnings and impacts.[239]

Moreover, the secrecy surrounding the algorithms and mathematical formulas used to create credit and consumer scores establish further obstacles to proving discrimination claims regarding these scores.[240] The mathematical models behind the scores are "trade secrets," or proprietary intellectual property, and therefore remain a mystery to regulators and the public.[241] For example, the Fair Isaac Corporation that compiles FICO scores does not publish its mathematical formula and consumers have no access to this information despite the power that FICO scores have on consumers' credit access and rates.[242]

In addition, the algorithms that drive consumer scores and segmentations are difficult to regulate because they are subject to change as data brokers gather further intelligence and change their models based on a broad range of factors and emerging innovations. Furthermore, subtle discrimination easily persists based on economic or historical data, and it is tough to show that the data is the result of continuing structural biases.[243] Furthermore, economists,

---

239. *See generally* Robert G. Schwemm & Jeffrey L. Taren, *Discretionary Pricing, Mortgage Discrimination, and the Fair Housing Act*, 45 HARV. C.R.-C.L. L. REV. 375 (2010) (discussing difficulty of proving discrimination in mortgage cases and the role of "discretionary pricing").

240. *See generally* Robert Unikel, *Bridging the "Trade Secret" Gap: Protecting "Confidential Information" Not Rising to the Level of Trade Secrets*, 29 LOY. U. CHI. L.J. 841 (1998) (noting how trade secrets law impedes regulation).

241. *See* UNIF. TRADE SECRETS ACT § 1 cmt. at 5-7 (amended 1985) (setting forth the trade secrets law that has been adopted in forty-seven states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands).

242. *See Scores – Scoring and Scoring Solutions*, FAIR ISAAC CORP., https://web.archive.org/web/20140214065800/http://www.fico.com/en/solutions/scores-scoring-and-scoring-services/ (last visited Jan. 27, 2015). There are also numerous blogs and online articles highlighting the secrecy of these scoring models as trade secrets. *See, e.g.*, Jason Steele, *How FICO Scores Are Calculated* (Feb. 24, 2012), http://www.investopedia.com/financial-edge/0212/how-is-fico-calculated.aspx.

243. Ann C. McGinley, *Discrimination Redefined*, 75 MO. L. REV. 443, 443-44 (2010) (highlighting persistence of discrimination at the "subtle level" and difficulty of proving discrimination claims under Title VII, especially with respect to gender); Deval L. Patrick, Robert M. Taylor, III & Sam S.F. Caligiuri, *The Role of Credit Scoring in Fair Lending Law–Panacea or Placebo?*, 18 ANN. REV. BANKING L. 369, 386-89 (1999) (noting how the difficulty of proving lending discrimination has left it to the U.S. Department of Justice to enforce fair lending laws, and that the Department has had to focus most of its limited resources on disparate treatment cases with respect to race).

policymakers, and even the general public, have come to accept price segmentation and differentials as reasonable means for companies to set prices based on market risk and demand.[244]

D. State Legislative and Enforcement Action

Many states have versions of the FCRA, and state attorneys general have asserted their own enforcement actions. However, some states have been more proactive in pursuing legislation targeting data brokers on broader levels. For example, a bill is under consideration in California in response to a court ruling that California's Song–Beverly Credit Card Act of 1971, which limits the data that merchants may retain about credit-card transactions, does not apply to online purchases and digital downloads.[245] In the case behind the court ruling, a consumer sued Apple for requiring personal information in violation of the Song–Beverly Act.[246] The court found that the text of the bill suggested that it applies only to physical stores.[247]

The California bill under consideration thus seeks to extend state law limitations on data collection to cover electronic purchases.[248] The bill essentially replicates the text of the Song–Beverly Act and adds language to include credit card transactions involving digital and downloadable products.[249] Accordingly the bill makes it illegal to record personal information with respect to purchases in-store or online. Merchants may only collect such information to the extent necessary for completing a transaction or for other permissible purposes such as fraud or identity theft prevention.[250] Nonetheless, even in these narrow circumstances,

244. *See generally* Anja Lambrecht et al., *Price Discrimination in Service Industries*, 23 MARKETING LETTERS 423 (2012).

245. S.B. 383, 2014 Leg., Reg. Sess. (Cal. 2014); *California Senate Approves Online Credit Card Privacy Bill*, PR NEWSWIRE (Jan. 30, 2014), http://www.prnewswire.com/news-releases/california-senate-approves-online-credit-card-privacy-bill-242841641.html. The Senate passed SB-383 on January 30, 2014, and it was ordered to the California General Assembly. It was read, and then referred to the Assembly Banking and Finance Committee on April 24, 2014. Cal. S.B. 383.

246. Apple Inc. v. Superior Court, 292 P.3d 883, 884 (Cal. 2013); CAL. CIV. CODE. §§ 1747-1748.95 (West 2009).

247. *Id.*

248. Cal. S.B. 383.

249. *Id.*

250. *Id.* § 3(c)(3)(A).

companies must destroy collected information as soon as the permissible purpose has been met.[251] Furthermore, the bill also bars companies from aggregating collected information or selling it to others.[252]

Notably, the bill is quite narrow in that it only applies to product purchases made "by any means of download to a computer, telephone, or other electronic device."[253] This means that the bill would not apply with respect to the use of a credit card to get a cash advance or make a security or damage deposit. It also would not apply to data collection related to delivering or installing special orders. In addition, online merchants could continue to collect consumer data with respect to purchase of downloadable products if the consumers opt in to data sharing.[254]

Opponents of the bill argue that it "places over-reaching restrictions on operators of commercial Internet Web sites or Online Services."[255] They argue that the bill imposes undue burdens on covered merchants by requiring that they notify consumers of the purpose of their requests for data and use of the information.[256] Some merchants also complain that the bill would thwart efficiency by requiring them to give consumers an opportunity to opt out of data collection at the outset of a transaction and again before the transaction is final.[257] Some critics also argue that the bill hinders merchants in seeking to protect consumers from identity theft despite its limited allowance for data collection to prevent fraud.[258]

In addition, the California Chamber of Commerce suggested that the bill would impose an "enormous burden[] on online retailers of digital products because it would require companies to bifurcate their digital product offerings into two categories depending on the amount of information shared by the consumer."[259] The Chamber further argues that the bill unduly hinders merchants' ability to notify

---

251. Cal. S.B. 383.

252. *Id.*

253. *Id.* § 2(p) (emphasis omitted).

254. Cal. S.B. 383.

255. S. RULES COMM., BILL ANALYSIS: THIRD READING 9 (May 7, 2013), *available at* http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_0351-0400/sb_383_cfa_20130528_131545_sen_floor.html.

256. *Senate Passes Bill Limiting Fraud Protection Efforts*, CAL. CHAMBER COM. (Feb. 6, 2014), http://www.calchamber.com/headlines/pages/02062014-senate-passes-bill-limiting-fraud-protection-efforts.aspx.

257. *See* Cal. S.B. 383 § 3(d)(3)(B).

258. S. RULES COMM., *supra* note 255, at 8-9.

259. *Senate Passes Bill Limiting Fraud Protection Efforts*, *supra* note 256.

consumers about software updates and upgraded pricing, and presents obstacles to their provision of other online support.[260] The Chamber adds that the bill will harm California-based Internet businesses by inciting class actions and requiring that there be a separate system for California consumers.[261]

In contrast to California, other states' consumer protection laws have been less aggressive in targeting data brokers. For example, Colorado's consumer protection law is narrower in its coverage. It prohibits merchants from collecting and retaining a consumer's entire credit card number and expiration date after a transaction is completed.[262] The law also prohibits merchants from recording a social security number (SSN) as identification or proof of creditworthiness.[263] A merchant nonetheless may record a credit card number when a check is issued to pay the amount due on that credit card, and may record a SSN on a loan application or on a check issued to pay a student loan.[264]

Colorado law also provides additional protections for SSNs more generally. The Colorado Consumer Protection Act states that a "person or entity" may not publicly post or display an individual's SSN, print a SSN on any card required to access products or services, or require an individual to transmit his or her SSN over an insecure connection on the Internet, unless the SSN is encrypted.[265] Furthermore, the law protects individuals from having to use their SSN to access an Internet web site without a password or unique personal identification number.[266] The law also prohibits entities from printing a "SSN on any materials that are mailed to the individual, unless state or federal law requires . . . or authorizes the SSN to be mailed."[267] The law nonetheless allows SSNs to (1) be included inside "applications and forms sent by mail"; (2) "establish, amend, or terminate an account, contract, or policy"; or (3) "confirm

260. *Id.* However, the bill specifically allows for data collection to establish, maintain and upgrade consumers' accounts. Cal. S.B. 383.

261. *Senate Passes Bill Limiting Fraud Protection Efforts*, *supra* note 256.

262. *See* COLO. REV. STAT. § 4-3-506 (2013) (adding that a merchant may record the type of credit card and the issuer of the credit card when a consumer displays a credit card as an indication of creditworthiness or identification).

263. *Id.* § 4-3-506(a).

264. *Id.* § 4-3-506(b).

265. *Social Security Numbers*, COLO. ATT'Y GEN., http://www.coloradoattorneygeneral.gov/initiatives/identity_theft/social_security_numbers (last visited Jan. 7, 2015).

266. *Id.*

267. *Id.*

the accuracy of the SSN."[268] However, SSNs in these mailings may not be printed on a postcard or otherwise visible on or through an "envelope or without the envelope having been opened."[269]

States also have brought enforcement actions regarding the use of data to engage in discriminatory practices to target particular groups. For example, in *State ex rel. Miller v. Vertrue, Inc.*, the Iowa Attorney General used statistical analysis to show that "Vertrue's marketing practices disproportionately affected elderly Iowans" in selling memberships in savings programs.[270] The state cross-referenced Vertrue's marketing information "with motor vehicle division, social security, and background investigation databases" to show how the company's deceptive marketing practices disproportionately impacted older consumers.[271] The court thus dismissed Vertrue's arguments that "it did not direct its marketing plans at the elderly, and programs were not designed to appeal to a specific age group."[272] The court found that even the company's own internal report noted the disproportionately high percentage of customers over fifty-five who purchased the deceptive plan at issue, and thus "Vertrue, at the very least, should have known that their fraudulent strategies disproportionately affected the elderly."[273]

Such cases are nonetheless rare. As noted above, it is very difficult to prove discriminatory data practices. Data brokers can generally "blame" discrepancies on the economics or other complexities of the market. Furthermore, the secrecy surrounding consumer scores create a nearly insurmountable hurdle for any would-be complainants to gather the evidence they would need for a successful claim. Still, policymakers are exploring the discrimination and data privacy concerns surrounding consumer scores and segmentations, and appear poised to propose or promulgate regulations.

III. ROADMAP TO REGULATIONS

Consumers have become increasingly concerned with their data privacy. Companies scoop up surprising amounts of information about consumers with little accountability. The Obama

268. *Id.*
269. *Id.*
270. 834 N.W.2d 12, 18, 44 (Iowa 2013).
271. *Id.* at 44.
272. *Id.*
273. *Id.* at 45.

administration has therefore proposed a privacy "bill of rights" to increase transparency regarding data brokers' collection and use of consumer data, and give consumers greater control over how companies use this personal information.[274] Furthermore, the FTC has highlighted data privacy and scoring concerns affecting consumers, and seeks to explore how Big Data affects low income and underserved consumers.[275] Indeed, this is an expansive issue. Accordingly, although companies and consumers derive benefits from data collection, its use in assessing secret scores and segmenting society creates public and private harms that policymakers should address with an aim toward advancing just policy.

A. Balancing Benefits and Burdens

Do consumer scores and segmentations merely facilitate benign business or foster discriminatory practices that deserve policy attention? Information asymmetries are not new in the B2C market. Consumers usually have less information than merchants regarding any given transaction and related privacy practices.[276] Indeed, consumers generally do not realize that data brokers track their every move, let alone that brokers use this data to determine what offers and deals consumers receive.[277] Data brokers usually do not notify consumers that they are gathering the consumers' data in order to assign consumer scores, and brokers certainly do not reveal or publicly explain the mathematical formulas or other trade secrets that drive these scores.[278]

Consumers benefit when they blissfully enjoy beneficial deals, fraud prevention, and innovative offerings due to the growth and depth of Big Data.[279] Companies benefit from data brokers' marketing services and assistance in boosting their bottom lines and

---

274. *See* Alexis, *supra* note 31 (internal quotation marks omitted).

275. *FTC to Examine Effects of Big Data on Low Income and Underserved Consumers at September Workshop*, *supra* note 34 (announcing the September 2014 workshop to explore these issues).

276. *See* Cullerton, *supra* note 19, at 819-20 (discussing "'information inequality'" among Jeroen van den Hoven's transparency concerns).

277. *Id.* at 819 (highlighting a story of a consumer who suffered a credit downgrade most likely due to his use of a credit card at Walmart, although that was merely an educated guess because the consumer did not have access to specific information underlying the downgrade).

278. *See id.*

279. RAMIREZ ET AL., *supra* note 1, at 47-48.

enhancing consumers' online experiences.[280] Companies also should have choice in contracting partners. Freedom of contract remains a backbone of commercial and contract law. Meanwhile, data brokers understandably guard their algorithms and models behind consumer scores as their proprietary business assets they have created through significant research and development.[281]

Nonetheless, overreliance on data-based practices and assumptions can also harm companies.[282] Rigid reliance on data and application of analytics may lead to poor marketing, hiring, and retention decisions and policies.[283] This is because such reliance on data ignores the humanity and fluidity of the market.[284] Indeed, "humans are messy and irrational," but data-driven determinations rely on assumptions that overlook this messiness.[285] Successful company leaders seek "'the elusive sweet spot between data truth and human truth.'"[286] They know that people and their interests change, and companies must embrace creativity and a growth mentality in order to prosper in an evolving market.[287]

For example, a zip code considered less desirable may quickly become a popular area inhabited by plenty of consumers who would be lucrative customers. However, companies reliant on consumer scores based on old assumptions about that zip code may ignore these consumers or offer them lesser deals. Data does not always drive the best marketing policies. Open-mindedness is important, and "a large measure of beyond-the-numbers insight is required to move past the bits and bytes so easily gathered with today's technology."[288]

---

280. *See id.* at 47.

281. *Id.* at 42.

282. *See* Rich Karlgaard, *Forget Piketty—Data Fascism Is the Bigger Threat*, FORBES (May 7, 2014, 6:00 AM), *available at* http://www.forbes.com/sites/richkarlgaard/2014/05/07/forget-piketty-data-fascism-is-the-bigger-threat (explaining how overreliance on data analytics can harm companies).

283. *Id.*

284. *Id.*

285. *Id.*

286. RICH KARLGAARD, THE SOFT EDGE: WHERE GREAT COMPANIES FIND LASTING SUCCESS 13 (2014) (quoting Robert Egger, chief designer of Specialized Bicycles). Karlgaard calls this "taste" and explains how this is a pillar of the "soft edge" central for companies' success. *Id.* at 150-72 (discussing taste).

287. *See id.* at 53-72. Basing decisions on assumptions derived from data underestimates the changing and often irrational nature of humanity. *Id.* at 17-18.

288. *Id.* at 169. Big Data does greatly benefit businesses by informing them of how individuals are using products and how they behave in the marketplace. *Id.* at 171. However, algorithms often need tweaking and lazy reliance on historical data leads businesses to become stagnant and miss opportunities. *Id.*

Furthermore, data-driven scores and segmentation may harm consumers.[289] Data-based assumptions may exacerbate class disparities by favoring the wealthy and sophisticated consumers to the disadvantage of the most vulnerable populations.[290] Algorithmic classifications skew how companies treat consumers and foster discrimination when based in part on assumptions related to race, gender, ethnicity, zip codes, and other data points that consider economic and educational resources.[291] These classifications increase the gaps between consumer "haves" and "have-nots" by leading companies to offer the "haves"—but not the consumer "have-nots"—the best offers and remedies.[292]

In addition, as noted above, current discrimination law is limited and largely ineffective in preventing or stopping discriminatory scoring and classification.[293] Reporting law also is essentially nonexistent with respect to scores used for marketing, and it is very difficult for consumers to learn about, let alone prove, discriminatory practices. Claimants face a tough burden in gathering data and trying to prove disparate treatment, and usually are unable to show disparate impact.[294] Moreover, it is especially difficult to prove discrimination with respect to consumer scoring due to its protection under trade secret law and the multifaceted data behind these scores.[295]

Consumer classifications also may not target minorities per se but nonetheless harm consumers under the guise of valid

289. Joseph W. Jerome, *Buying and Selling Privacy: Big Data's Different Burdens and Benefits*, 66 STAN. L. REV. ONLINE 47, 50 (2013).

290. *Id.* at 51 (further explaining that "[m]ost of the biggest concerns we have about big data—discrimination, profiling, tracking, exclusion—threaten the self-determination and personal autonomy of the poor more than any other class").

291. *See id.*

292. *Id.* at 50-52; *see also* Jonas Lerman, *Big Data and Its Exclusions*, 66 STAN. L. REV. ONLINE 55, 55 (2013) (also noting how Big Data fails to capture the preferences and risks for those that do not actively engage with data).

293. Cullerton, *supra* note 19, at 820-23 (emphasizing how consumer scores may amount to discrimination).

294. *See, e.g.*, Carle, *supra* note 237, at 297-98 (noting the difficult burden to bring a disparate impact case); Plummer v. W. Int'l Hotels Co., 656 F.2d 502, 505 (9th Cir. 1981) ("A civil rights plaintiff has a difficult burden of proof, and should not be deprived of what may be persuasive evidence." (footnote omitted)).

295. Reddix-Smalls, *supra* note 13, at 100-18 (noting the secrecy of credit scores and dangers of algorithms); Unikel, *supra* note 240, at 841-90 (discussing concerns regarding use of trade secrets law to impede regulation).

marketing.[296] For example, a data broker's classification of a consumer as a "Biker Enthusiast" based on inferences from data collected online and offline may benefit the consumer when used by a motorcycle dealership for targeted marking.[297] However, this classification may hurt that consumer when an insurance company uses it to infer risky behavior.[298] Similarly, a consumer may enjoy receiving sugar-free candy coupons due to data suggesting that the consumer has a "Diabetes Interest," but suffer higher insurance rates due to that same categorization.[299] Worse yet, these consumers generally are unaware of these classifications or their impacts and have no means for contesting their veracity or precluding their use.[300]

While some condone this as usual marketing, it fosters inequities and hinders consumers' trust in the marketplace.[301] Such injustice also may spread in communal ways and violate relational norms. Taken to its extreme, scoring based on one's social connections or "friends" on Facebook creates incentive to avoid companions and family with less advantageous economic, social, or professional profiles. Consumers should not be essentially punished based on who their friends are. This seems to offend basic morality and asks for consumers to base their social networks on creditworthiness instead of kindness, love, and familial ties.[302]

B. Proposed Reforms

Most policymakers and commentators have focused on need for consumer notice that their data is being collected and giving them choice regarding such data collection.[303] They target data brokers' practices and urge them to give consumers the power to learn about and stop data collectors' overreaching.[304] FTC Commissioner Brill's

296. RAMIREZ ET AL., *supra* note 1, at 48-49 (highlighting the pros and cons of consumer scoring and classifications).

297. *Id.* at 49 (providing the example).

298. *Id.* at 48 (providing the example).

299. *Id.* (providing the example).

300. *Id.*

301. *Id.*

302. *See* Cullerton, *supra* note 19, at 826-28 (discussing how consumer scores may harm relational norms).

303. This may be due in part to the data industry's indication that it would prefer such a self-regulatory regime over more intrusive regulations, such as broad bans on data collection. Solove & Hartzog, *supra* note 201, at 590–94 (noting how privacy policies emerged).

304. Brill, *supra* note 198, at 10.

"Reclaim Your Name" initiative, the proposed Data Broker Accountability and Transparency Act of 2014 (DATA Act), and the most recent FTC proposals reflect this agenda.[305]

1. *Reclaim Your Name*

FTC Commissioner Brill has announced a comprehensive initiative called "Reclaim Your Name" aimed at enhancing consumer choice with respect to data collections.[306] As she stated in her 2014 presentation at Princeton University:

> I believe we need to improve our commercial privacy laws in the US. I believe Congress should enact three pieces of legislation to help address these issues. First, I call on Congress to enact legislation that would require data brokers to provide notice, access, and correction rights to consumers scaled to the sensitivity and use of the data at issue. Such a law should require data brokers to give consumers the ability to access their information and correct it when it is used for eligibility determinations, and the ability to opt-out of information used for marketing. . . . Second, I believe adoption of baseline privacy legislation for the commercial arena would close the gaps in consumer privacy protections and help level the playing field among businesses. And third, I think it is increasingly clear that the United States needs data security legislation.[307]

As an initial step in the direction of enhanced notice and choice, this agenda would involve creation of a single portal for consumers to gain control over the information collected about them.[308] The portal would thus "give consumers the power to access online and offline data already collected, exercise some choice over how their data will be used in the commercial sphere, and correct any errors in information being used by those making decisions seriously affecting consumers' lives."[309] The portal also would educate consumers about companies' privacy policies by stating the facts in simple and straightforward language instead of the incomprehensible legalese that obfuscates most companies' privacy policies.[310] This movement has been central in the FTC's data privacy agenda,[311] and

305. *Id.* at 9.
306. *Id.* at 8.
307. *Id.*
308. *Id.* at 9.
309. *Id.*
310. *Id.*
311. *See* Julie Brill, *Demanding Transparency from Data Brokers*, WASH. POST (Aug. 15, 2013), http://articles.washingtonpost.com/2013-08-15/opinions/41412540_1_data-brokers-fair-credit-reporting-act-data-fuel; Julie Brill, Comm'r, Fed. Trade Comm'n, Reclaim Your Name, Keynote Address at 23rd Computers Freedom

Commissioner Brill again voiced support for similar policy initiatives in her statement on May 27, 2014.[312]

2. *Data Broker Accountability and Transparency Act of 2014 (DATA Act)*

Similarly, Senators Jay Rockefeller (D-W.Va.) and Ed Markey (D-Mass.) introduced the DATA Act to codify many of the same data privacy and choice provisions.[313] The bill has been assigned to the Committee on Commerce, Science, and Transportation, where it remains for consideration before possible presentation to the House or Senate as a whole.[314] This Act would bar data brokers from obtaining or attempting to obtain information that a data broker knows or should know to be stolen or false, unless the information is collected to identify a discrepancy.[315] It also would require that data brokers establish procedures to ensure the accuracy of information that specifically identifies an individual, unless the information only identifies a name or address.[316]

In addition, the DATA Act would require data brokers to allow consumers to review personal information gathered about them at least one time per year, free of charge.[317] Consumers would then have power to dispute the accuracy of the data collected, and the data brokers would have to investigate disputes and correct any erroneous information.[318] The DATA Act also would empower the FTC to establish the aforementioned website with information about consumers' privacy rights and how consumers may review personal information and object to its use for marketing purposes.[319] The FTC also would promulgate regulations to implement and enforce the DATA Act and ensure that data brokers create measures to audit internal or external access to information they collect.[320]

---

and Privacy Conference (June 26, 2013), *available at* http://www.ftc.gov/speeches/brill/130626computersfreedom.pdf.

312. RAMIREZ ET AL., *supra* note 1, app. at C-3–C-8 (providing an additional statement of Commissioner Julie Brill with the May report).

313. Data Broker Accountability and Transparency Act, S. 2025, 113th Cong. (2014).

314. *Id.*

315. *Id.* §§ 3(a)-4(b)(1).

316. *Id.* § 4(a).

317. *Id.* § 4(c)-(d).

318. *Id.* § 4(f).

319. *Id.* § 5(2).

320. *Id.* § 5.

A violation of the DATA Act would be a violation of the FTC Act.[321] Accordingly, the FTC could pursue violators and subject them to related penalties. State attorneys general and other state agencies also would have power to enjoin further violations, compel compliance, obtain damages on behalf of residents of their states, and obtain civil penalties in an amount no greater than $16,000 per violation.[322] However, these state actors would have to refrain from instituting a civil action during the pendency of any FTC action.[323]

3. *The FTC's May 2014 Proposal*

After the DATA Act's introduction, the FTC highlighted its support for much of the Act's provisions in its May 2014 data broker report.[324] The FTC echoed the DATA Act in recommending legislation requiring free consumer access to collected information at least once per year and means for "opting out" of data collections.[325] The FTC also reinforced the DATA Act's and Commissioner Brill's proposed creation of a central website for identification of data brokers and links to data brokers' access tools and opt-outs with respect to data sharing for marketing purposes.[326] The FTC also urged establishment of measures for auditing or retracting any internal or external access to data containing collected personal information.[327] The FTC added that the law should require that consumers must *opt in* to allow any data sharing of *sensitive* information, such as that related to health issues.[328]

The FTC's proposed legislation would nonetheless differ from the DATA Act in various ways. For example, the FTC suggested that the Internet portal requirements should be limited to the largest fifty data brokers in order to advance its efficacy and help minimize information overload.[329] The FTC also proposed that data brokers list clients to whom they distribute collected data and disclose inferences they derive from such data (such as an inference that a consumer is

321. *Id.* § 6(a).
322. *Id.* § 6(e)(1)-(2).
323. *Id.* § 6(e)(3)(C).
324. RAMIREZ ET AL., *supra* note 1, at 49-56 (discussing proposed legislation).
325. *Id.* at 54.
326. *Id.* at 50.
327. *Id.* at 53-54.
328. *Id.* at 50-54 (adding further detail regarding such proposed legislation).
329. *Id.* at 51.

interested in a certain activity based on Internet search history).[330] Additionally, the FTC's proposed legislation would require data brokers to notify consumers when collected data adversely impacts a consumer transaction or prevents a consumer from a potential benefit.[331]

The Commission's recommendations also went further to propose privacy by design.[332] This would employ logarithms and software with privacy features that limit data collection to information essential for a particular transaction and preclude data collection with respect to youth under eighteen years of age.[333] The FTC urged that such measures would augment the Children's Online Privacy Protection Act's (COPPA) protections of children's privacy by extending restrictions to data collected offline.[334] In addition, the FTC called on data brokers to establish measures for ensuring that downstream users of data do not use the data for discriminatory or other unlawful eligibility determinations with respect to credit, insurance, or employment.[335]

It is nonetheless unclear how the FTC's legislation or the DATA Act would work, or whether such regulations' benefits would outweigh their costs. For example, the FTC's report noted the Commissioners' disagreement on creation of an opt-out portal due to such costs.[336] Commissioner Wright voiced concern that the benefits to consumers of requiring data brokers to provide them with the ability to opt out of data sharing for marketing purposes may not outweigh the costs of imposing such restrictions on companies.[337] The report further explained that

> although the concept of a centralized portal to provide consumers with information about the practices of data brokers may be useful in theory,

---

330. *Id.* at 52.

331. *Id.* at 53-54. The DATA Act does not require disclosure of inferences made from collected data, the names of clients who purchase data, or sources of data if the data adversely impacts a consumer transaction or potential benefit. *See* Data Broker Accountability and Transparency Act, S. 2025, 113th Cong. (2014). The DATA Act does not protect offline data collection from youth under the age of 18, as proposed by the FTC's recommendation. *Id.* The DATA Act also does not require "privacy by design" methods in creating data systems to ensure downstream users do not use data for unlawful or discriminatory purposes. *Id.*

332. RAMIREZ ET AL., *supra* note 1, at 54.

333. *Id.* at 55.

334. *Id.*

335. *Id.* at 55-56.

336. *Id.* at 50 n.82.

337. *Id.* at 51 n.85.

> [Commissioner Wright] believes that the Commission should engage in a rigorous study of consumer preferences sufficient to establish that consumers would likely benefit from such a portal prior to making such a recommendation.[338]

The FTC's proposed website portal would be limited to the fifty largest data brokers, but delineating that list could be problematic.[339] Furthermore, the proposal does not clarify the scope of data that the regulations would cover, or address consumers' inertia when it comes to their contracts and privacy. Most consumers already lack interest in reading their contracts and verifying their credit reports. It is therefore unlikely that the majority of consumers would invest the time and resources required to review all information collected and verify its accuracy. Instead, only the most resourceful and sophisticated consumers would take on this task—possibly increasing the gap between the consumer "haves" and "have-nots."

It is also questionable that creating a system similar to that under the FCRA would improve the accuracy of data collections. With respect to credit reports, policymakers have proposed the Stop Errors in Credit Use and Reporting (SECURE) Act to address rampant inaccuracies in credit reports and scores by increasing and expanding the requirements on credit reporting agencies and data furnishers.[340] U.S. Senators Sherrod Brown (D-OH) and Brian Schatz (D-HI) proposed this act in the wake of a Consumers Union report indicating that credit report errors affect 40 million Americans and can devastate consumers who face significant obstacles in seeking to correct these errors.[341] Senator Schatz endorsed the act, emphasizing that tougher measures are necessary to combat "a dark ecosystem of

338. *Id.*

339. *Id.* at 51 n.86. The FTC suggested that "large data brokers" could be defined through rulemaking like the CFPB has done to determine "larger participants" subject to its examination authority under 12 U.S.C. § 5514(a)(1)(B). *Id.* However, such rules leave gaps and it seems especially difficult with respect to data brokers due to the breadth, depth, and variability that have been hallmarks of the Big Data industry. Arguably every company could be considered a data broker in some respects.

340. *Sens. Brown and Schatz Announce Legislation Protecting Consumers from Inaccurate Credit Reports and Scores*, BROWN (Apr. 9, 2014), http://www.brown.senate.gov/newsroom/press/release/sens-brown-and-schatz-announce-legislation-protecting-consumers-from-inaccurate-credit-reports-and-scores [hereinafter *SECURE Act Press Release*].

341. *Id.*

companies that are not accountable to consumers" despite their tremendous power in determining consumers' credit[342]

Specifically, the SECURE Act would provide consumers with free credit scores and empower the CFPB to develop procedures for credit reporting agencies to follow as a means to improve accuracy.[343] It also would require credit reporting agencies to send creditors the materials related to consumer disputes and facilitate effective resolution of these disputes.[344] Sponsors emphasized that this is especially important to address the reported failures in current dispute resolution procedures.[345] The Act also would empower courts to stop a credit reporting agency from reporting inaccurate information and provide the FTC with increased authority to bar reporting agencies' poor practices.[346]

C. Balanced Change

Policymakers, academics, and consumer advocates are encouraging the data broker industry to take more aggressive action to protect consumer privacy. It is unlikely, however, that companies with a monopoly on data collection will take socially optimal action on their own.[347] Moreover, legislative or regulatory action is warranted to address public harms emanating from unchecked consumer scoring and segmentation. As the WPF concluded:

> Consumer scoring has substantial potential to become a major policy issue as scores with unknown factors and unknown uses and unknown validity and unknown legal constraints move into broader use. Secrecy, fairness of the factors, accuracy of the models, and the use of sensitive information are some of the key issues that must be addressed. It is exquisitely unlikely that self-regulation will solve all of the dilemmas consumer scoring introduces.[348]

---

342. *Id.*

343. SECURE Act, S. 2224, 113th Cong. § 3(e)-(f) (2014); *SECURE Act Press Release*, *supra* note 340.

344. *SECURE Act Press Release*, *supra* note 340.

345. *Id.*

346. *Id.*

347. *See* Daniel P. O'Brien & Doug Smith, *Privacy in Online Markets: A Welfare Analysis of Demand Rotations* 36-38 (Fed. Trade Comm'n Bureau of Econ., Working Paper No. 323, 2014), *available at* http://www.ftc.gov/system/files/documents/reports/privacy-online-markets-welfare-analysis-demand-rotations/wp323.pdf (assessing the transactional costs associated with data privacy practices and protections, and arguing that effective competition is one tool that would assist socially beneficial privacy choices).

348. DIXON & GELLMAN, *supra* note 7, at 84.

Therefore, the time is ripe to craft regulations that are workable and efficient, but sufficiently robust to address scoring's and segmentation's perpetuation of unfair assumptions and ultimately discrimination. This should begin with cost-effective notice and choice regulations backed by enforcement and dispute resolution mechanisms that prompt data brokers to honor consumers' privacy preferences. It also should include strong auditing procedures that hold data brokers accountable for discriminatory or otherwise improper use of consumers' data.

1. *Notice and Choice*

Currently, companies often include their privacy policies in the fine print of their contracts, but such weak disclosure is largely meaningless because consumers rarely read these contracts or launch successful privacy claims based on contract or tort law.[349] Furthermore, some companies do not even have privacy policies.[350] The FTC has had to rely mainly on creation of "soft law" through reports, workshops, guidelines, and settlement decrees with respect to the enforcement actions it has pursued.[351]

Accordingly, creation of a notice and choice portal like that proposed by the DATA Act and the FTC's report is a step in the right direction toward advancing more meaningful transparency. This also would comport with most commentators' and courts' support for disclosure laws that protect freedom of contract while making consumers responsible for reading contracts and making appropriate choices.[352] It is thus no surprise that regulators advocate for greater disclosure regarding consumers' data profiles.[353] This type of notice and choice also helps to balance the power in B2C transactions and interactions.

Nonetheless, such notice and choice is not sufficient to address discriminatory effects of consumer classifications and segmentations

349. Solove & Hartzog, *supra* note 201, at 591-96. The article emphasizes that '"broad statements of company policy do not generally give rise to contract claims'" and that tort claims similarly have failed. *Id.* (quoting Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004)).

350. *See id.* at 588.

351. *Id.* at 625-27 (explaining the creation of soft law that is not enforceable per se but persuasive through various means short of specific rulemaking).

352. *See, e.g.*, Robert A. Hillman & Maureen O'Rourke, *Defending Disclosure in Software Licensing*, 78 U. CHI. L. REV. 95, 105 (2011).

353. Cynthia Dwork & Deirdre K. Mulligan, *It's Not Privacy, and It's Not Fair*, 66 STAN. L. REV. ONLINE 35, 36 (2013).

produced by big data analysis.[354] Instead, giving individuals notice and choice may simply perpetuate the growing gap between consumer "haves" and "have-nots" because the least sophisticated consumers remain least likely to protect themselves.[355] As noted above, consumers already lack the education, resources, and time required to read the usually long and laborious fine print of their contracts, thus making it difficult to imagine that they would have the wherewithal to access many companies' privacy policies and opt out.[356]

Information overload also may drive even the sophisticated consumers who comprehend privacy policy terms to nonetheless take no action to protect their privacy. An opt-out portal with overly abundant disclosures and options would overwhelm consumers, leading them to make no choices due to confusion, exhaustion, and lack of patience. Consumers also are apt to be overly optimistic and assume that companies will interact with them in a fair manner.[357] They also may assume that they would be sufficiently savvy to detect and deal with any unsavory or problematic contract terms.[358]

Furthermore, data devices like cookies could render an opt-out portal ineffective.[359] For example, the researchers from Berkeley noted above argue that any opt-out rules must be accompanied by restrictions on companies' use of cookies that reinstate themselves after deletion as means for circumventing consumers' data choices.[360] They further suggest that companies should disclose how they enhance the information a consumer provides with information purchased or secured by outside trackers.[361]

---

354. Dwork & Mulligan, *supra* note 353, at 36.

355. *See id.* at 36-38. Big Data is essentially a "sociotechnical system" that should be regulated with balanced regulations crafted by policymakers, lawyers, technologists, and other stakeholders with a focus "on the risks of segmentation inherent in classification." *Id.* at 38-39.

356. Tess Wilkinson-Ryan, *A Psychological Account of Consent to Fine Print*, 99 IOWA L. REV. 1745, 1751-70 (2014); *see also* Skelton v. Gen. Motors Corp., 660 F.2d 311, 313-14 (7th Cir. 1981) (describing a statute's drafters' concern that "consumer product warranties often were too complex to be understood").

357. *See* Wilkinson-Ryan, *supra* note 356, at 1771.

358. *See id.* at 1771-74. *See generally* Schmitz, *supra* note 18 (further discussing psychology of consumer contracting).

359. *See supra* notes 55-69 and accompanying text (discussing robust cookies, third-party collections, and other technologies that threaten one's ability to protect herself online).

360. Hoofnagle et al., *supra* note 55, at 291-95.

361. *Id.* at 295.

As noted above, an Internet portal for disclosure and opting out of data collection also raises additional practicality and cost issues. What data falls within the scope of this requirement, considering how broad "marketing" may be construed? How much will the system cost for regulators and companies seeking to comply? Who will monitor the system, and where will the funding come from?[362] Again, will these costs and burdens outweigh any benefits of the system, considering that most consumers already lack time, resources, and patience to check their credit reports under the FCRA? Similar concerns underlie Commissioner Wright's noted objections to the FTC's proposed legislation.[363]

That said, increased transparency and access to collected information would help promote brokers' compliance with regulations and best practices. Many consumers would use the portal if it is easily accessible, understandable, and reasonably limited in scope. Accordingly, the portal could be limited more strictly than the FTC has proposed to include only the largest twenty or twenty-five data brokers. The portal should be sure to cover and highlight those data brokers who generate consumer scores or segmentations, especially those that factor in race, gender, income, and the like. In addition, industry fees or a tax on revenues from selling consumer data could cover the costs of the portal.

A limited portal would be more cost-effective and help protect the smaller businesses with lower revenues from data collections.[364] A more limited portal also would help minimize information overload, especially if portal designers are vigilant to provide a user-friendly interface for consumers. Additionally, it would be more manageable for regulators to monitor a more streamlined and simple portal. Again, the aim should be to provide a user-friendly notice and choice mechanism that provides the greatest "bang for the buck" in protecting consumers and alerting regulators of possibly discriminatory use of data.

---

362. The FTC's staff and funding are quite limited. *See* Solove & Hartzog, *supra* note 201, at 599-607 (noting that there were only forty-five staff in the FTC's Division of Privacy and Identity Protection in 2010).

363. *See supra* notes 329-39 and accompanying text (discussing the FTC's proposal and Commissioner Wright's concerns regarding this requirement).

364. Please note, nonetheless, that determining a "revenue" threshold is very difficult to begin with, and especially problematic with respect to data brokers with limited assets and ability to orchestrate accountings to bypass revenue limits. Moreover, these are merely initial ideas and further research and system design should follow. This Article seeks to merely open the discussion and inspire ideas.

2. *Enforceability Measures*

Furthermore, any portal of this kind should be backed by a dispute resolution process and measures for enforcing resolutions and consumer choices. Contract claims based on choices under privacy policies are generally futile.[365] It is usually not worth it for consumers to bring contract claims in light of litigation costs.[366] Furthermore, it is difficult to prove causation or the amount of damages with respect to data breaches or data inaccuracies.[367] That is especially true with respect to the emotional repercussions that often accompany a data breach.

Accordingly, any central data privacy portal should give consumers not only the ability to opt out of data sharing and access to the information collected about them, but also the power to hold the brokers accountable. This could be done efficiently through a complaint or online dispute resolution (ODR) system that ensures enforcement of opt-out choices and correction of proven data inaccuracies. As noted above, the SECURE Act has been proposed in part to address rampant errors in credit reports that go uncorrected due to lack of an effective dispute resolution system.[368] The same problems would likely plague any system with respect to data collections that is set up without a clear remedy system.

ODR systems are growing in popularity and offer cost-effective resolution of consumer disputes worldwide.[369] An ODR system could be linked with the central opt-out and disclosure portal. Through this link, consumers could efficiently pursue brokers who do not respect their data collection choices or correct data inaccuracies. This would allow consumers to use an online stepped process to obtain timely remedies. This could walk the parties through (1) negotiation; (2) mediation; and (3) arbitration as needed to ensure a speedy and final resolution based on the supporting documentation.

---

365. Solove & Hartzog, *supra* note 201, at 595-97.

366. *See id.*

367. *Id.* (noting failures of contract law to address data privacy issues, and using the failed contract claim of airline passengers who claimed misuse of their information after the September 11th attacks due to inability to prove damages).

368. *See supra* text accompanying notes 340-46 (discussing SECURE).

369. Amy J. Schmitz, *Introducing the "New Handshake" to Expand Remedies and Revive Responsibility in eCommerce*, 27 ST. THOMAS L. REV. (forthcoming 2014); Schmitz, *supra* note 18, at 319-31. *See generally* Amy J. Schmitz, *"Drive-Thru" Arbitration in the Digital Age: Empowering Consumers Through Binding ODR*, 62 BAYLOR L. REV. 178 (2010) (discussing the promise of and suggesting best practices for ODR).

Such an ODR system would differ from a general complaint process by bringing in a neutral third party to facilitate settlement pursuant to online mediation. It also would engage a third-party neutral to determine the merits of the complaint if the dispute is not settled by mutual agreement through negotiation or mediation. Furthermore, data brokers who do not follow timelines and procedures for investigating data breach claims, ceasing data collections, or correcting errors in accordance with the system, could be fined and/or subject to enforcement action. Additionally, the ODR mechanism would allow the FTC and other regulators to easily monitor data brokers' compliance while also providing consumers with enforced resolutions of their data disputes.[370]

This ODR system also could build from a complaint process like that employed by the CFPB with respect to financial products and service disputes.[371] The CFPB's complaint process has been effective in shedding light on improper credit card practices and has assisted the CFPB in focusing its enforcement efforts on companies with poor complaint records and industries fraught with consumer protection violations.[372] The complaint database also is publicly available, which allows consumers to investigate companies' track records and assists industries in learning what matters to consumers.[373]

However, such complaint processes still do not ensure that companies will reply to complaints or provide any redress.[374] Unlike the ODR process suggested above, general complaint processes do not culminate in a third-party determination on the merits if the parties fail to reach a mutual resolution.[375] Furthermore, general

370. Again, these are merely initial ideas. Further development and discussion is essential.

371. *See* CONSUMER FIN. PROT. BUREAU, CONSUMER RESPONSE: A SNAPSHOT OF COMPLAINTS RECEIVED JULY 21, 2011 THROUGH JUNE 30, 2014 (2014) [hereinafter CFPB REPORT], *available at* http://files.consumerfinance.gov/f/201407_cfpb_report_consumer-complaint-snapshot.pdf (analyzing consumer complaints filed according to different categories).

372. *Id.*

373. Ian Ayres, Jeff Lingwall & Sonia Steinway, *Skeletons in the Database: An Early Analysis of the CFPB's Consumer Complaints*, 19 FORDHAM J. CORP. & FIN. L. 343, 345-58 (2014) (discussing the purpose and process of the database).

374. *Id.* at 350-67 (noting untimely or inadequate responses to consumer complaints in particular industries).

375. *Id.*; CFPB REPORT, *supra* note 371. The CFPB has proposed adding consumer narratives to the complaint database to increase transparency. Disclosure of Consumer Complaint Narrative Data, 79 Fed. Reg. 42,765 (proposed July 23, 2014). They are testing the ability to scrub personal information from the narratives,

complaint processes do little to prevent companies from ignoring claims, as they have done with respect to claims asserted with the CFPB by minorities, elderly, and other vulnerable populations.[376] This again augments power imbalances and allows for businesses to discriminate in terms of the remedies and support they provide to different consumers. Accordingly, any complaint process must incorporate robust dispute resolution procedures and enforcement measures.

Of course, these are merely initial ideas for a cost-effective and beneficial enforcement system to support an opt-out portal, and further development is essential. Data brokers will likely resist such transparency and responsibility regulations, especially those that add to their costs. It is also unlikely that they will welcome rules that increase their vulnerability to FTC action. Nonetheless, some data brokers may embrace such regulations as means for weeding out those brokers that harm the industry's goodwill. Furthermore, the benefits of ODR would outweigh its costs, which could be spread among data brokers. Moreover, an ODR system that is free for all consumers would allow vulnerable consumers to obtain remedies and address problematic use of their data.

3. *Audits and Accountability Rules*

Opt-out and data-dispute measures that empower consumers to make enforceable choices and data corrections are an initial step in the right direction. Consumers should take responsibility in protecting themselves, and a central portal could (1) raise awareness about data collection and (2) increase brokers' accountability. However, such measures do not go far enough in addressing discriminatory effects of consumer scores and segmentation. Those with the least education and resources are still least likely to access and benefit from any central portal, even if it is more limited.

Accordingly, any legislation or regulations should include auditing and accountability measures that aim to stop and prevent improper and discriminatory use of data. This could begin with measures like those in DATA Act and the FTC's proposal that require brokers to establish procedures to ensure accuracy of data

---

and must consider the risk of re-identification of consumers. *Id.* at 42,767. It is also questionable whether adding this information would lead to information overload.

376. Ayres, Lingwall & Steinway, *supra* note 373, at 363-67 (finding in their study of the CFPB's complaint process that African-Americans and Hispanics faced untimely company responses, along with the elderly).

collection and legitimacy of data usage.[377] As the FTC has suggested, legislation also could promote "privacy by design" aimed to limit data collections to necessary information related to particular transactions and to protect vulnerable individuals such as youth under eighteen years of age.[378]

In addition, the FTC's proposed default rules precluding data sharing with respect to sensitive information could be coupled with additional duties to protect vulnerable consumers in traditionally disadvantaged groups.[379] Brokers also should be required to establish auditing and compliance measures aimed to catch discriminatory use of consumer information for consumer classifications and scoring.[380] Commissioner Brill noted need for stiffer legislation to address discriminatory use of data in her May 27, 2014 statement.[381] As she and the FTC have suggested, these measures could begin with requiring data brokers' due diligence in preventing discriminatory use of data they share and sell.[382]

As noted, some have suggested that the FCRA and ECOA should be extended to target discrimination regarding not only credit, employment, and insurance determinations, but also broader use of collected data.[383] However, these acts have not done enough to combat arbitrary assessments and disparate impacts of credit scoring.[384] Thus stronger auditing and enforcement measures are necessary for use of data for credit, as well as marketing determinations.[385]

---

377. *See supra* Subsections III.B.2-3 (discussing DATA ACT and the FTC's proposal).

378. *See supra* Subsection III.B.3 (discussing the FTC's proposal).

379. *See supra* text accompanying notes 324-28.

380. *See* Dwork & Mulligan, *supra* note 353, at 35-36.

381. RAMIREZ ET AL., *supra* note 1, app. at C-1, C-5, C-7 (providing an additional statement of Commissioner Julie Brill with the report).

382. *Id.*

383. *Id.*

384. *Id.*; *see also* Frank Pasquale & Danielle Keats Citron, *Promoting Innovation While Preventing Discrimination: Policy Goals for the Scored Society*, 89 WASH. L. REV. 1413, 1418-24 (2014) (responding to Professor Zarsky's critique of their *Scored Society* article and highlighting the dangers of scoring in light of the volume, velocity, and variety of information that can affect one's score).

385. *See* Citron & Pasquale, *supra* note 33, at 6-20 (exploring the opacity of credit scores and lack of meaningful insight over the credit reporting process, and proposing auditing trails and interactive modeling aimed to assist consumers in making decisions based on how it may impact their credit scores); Cullerton, *supra* note 19, at 820-24 (highlighting continued discriminatory use of data).

Accordingly, mandatory—and not merely suggested best practices—should require data brokers to conduct due diligence before selling or sharing consumer scores to ensure the accuracy of the information collected and assess whether would-be data purchasers use data classifications in a discriminatory manner.[386] Such rules also should require companies that buy consumer scores and segmentations to reasonably investigate the creation and accuracy of what they buy.[387] These companies should then be required to file simple reports regarding their use of data through an efficient online process.

This would place more responsibility on companies with respect to their direct and ongoing interactions with one another, instead of relying on consumers' pro-action. It thus would protect consumers' reasonable expectations without requiring that consumers vigilantly police onerous privacy policies.[388] Furthermore, it would remind data brokers on a periodic basis to check their own systems for improprieties. This could benefit companies by preventing them from facing expensive regulatory enforcement actions and consumer complaints or class actions that also harm their goodwill.[389]

Auditing procedures also could help regulators ensure the legitimacy of the automated decision-making systems that underlie consumer scoring and segmentations. Automated data collection and decision-making systems take human decision-making out of the process and are becoming the "*primary* decision makers" in B2C dealings without adherence to due process standards.[390] For example, automated systems have resulted in the unfair termination of individuals' Medicaid benefits, food stamps, and other welfare

386. *See* RAMIREZ ET AL., *supra* note 1, app. at C-5, C-7 (providing an additional statement of Commissioner Julie Brill with the report).

387. *See id.*

388. *See* Solove & Hartzog, *supra* note 201, at 627-76 (emphasizing need to protect consumers' expectations and how the FTC is already moving in that direction with its enforcement actions). It is simply unreasonable to expect consumers to access, understand, and act based on privacy policies—which companies may or may not employ.

389. *Id.* at 613. Again, it is true that reporting and auditing measures do increase costs for companies, perhaps requiring that they hire compliance officers. However, these costs could be minimized through simple online forms and awaken businesses' awareness of data breaches of improprieties—perhaps due to particular employees' poor practices.

390. *See* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1252-53 (2008).

benefits.[391] As another example, "Colorado's public benefits [automated] system . . . denied Medicaid to patients with breast and cervical cancer based on income and asset limits that were not authorized by federal or state law."[392] The opacity of automated systems behind consumer scoring and segmentations may thus deprive individuals' rights and property without appeal to human fairness.[393]

Of course, human decision-making also can harm consumers due to individuals' conscious and subconscious biases that affect their determinations. Still, regulations should subject automated consumer assessment systems to audits to help correct errors in the systems and prevent improper use of biases and assumptions from infecting their operations.[394] For example, regulators should audit systems that crunch collected data to determine classifications such as "Urban Scramble" or "Mobile Mixers" (noted earlier with respect to the FTC's study of Big Data).[395] Such determinations are based on not only collected data, but also questionable assumptions (i.e., inferring that a certain zip code connotes lower income or racial status).[396]

Understandably, such reporting and auditing requirements raise cost concerns. However, the costs of such compliance measures are not much more than those companies already may absorb under the

---

391. *Id.* at 1256-57. Automated processes ease public and private costs, but they also thwart policy when programmers translate complex data into code using "[c]omputer languages [that] may be unable to capture the nuances of a particular policy." *Id.* at 1257-65.

392. *Id.* at 1268-72 (noting individuals' reluctance to challenge automated systems due to "'automation bias'").

393. For example, digital analytics and processes have resulted in termination of Medicaid benefits, garnishment of wages, and placement on "No-Fly" lists. *Id.* at 1273-81 (internal quotation marks omitted).

394. *See id.* at 1301-13.

395. *See supra* text accompanying note 6 (discussing the FTC's finding regarding these suspect segmentations of Latinos and African-Americans built on collected data and inferences); Citron, *supra* note 390, at 1275-310 (discussing due process concerns regarding automated decision making).

396. One commentator has advocated for audits of automated decision making by public agencies (i.e., determination of government benefits) as means for addressing over-reliance on automated processes and encouraging critical assessment of computer's specific findings. Citron, *supra* note 390, at 1275-311. Private decision-making should not be subject to the same scrutiny as public determinations, but may nonetheless be open to regulations when possibly based on bias and unverified assumptions.

FTC's consent order process.[397] The FTC's consent orders often impose reporting and auditing requirements on data brokers, and require companies to notify "the FTC of any material changes in their organization[s] that [may] affect compliance."[398] Orders also may impose fines, independent audits, consumer notification and remediation, and establishment of data-integrity or security programs.[399] Legislative or regulatory auditing and reporting measures would merely broaden these duties beyond the relatively few brokers that are "caught" through enforcement actions.[400]

Furthermore, any financial costs are justified in light of social costs of discriminatory practices and brokers' profits from using consumers' data.[401] In addition, system expenses could be minimized through use of a simple online reporting portal and forms that focus on gathering what information and assumptions go into creating consumer scores and segmentations.[402] Regulators also could limit their resources to auditing brokers who create or use the most problematic scores and segmentations, and adding minimal random audits in order to incentivize companies' compliance.[403]

Reporting and auditing need not be draconian or overly intrusive. Companies should continue to use models that benefit consumers by allowing companies to offer goods and services tailored to consumers' wants and needs. However, outdated and shortsighted assumptions based on gender, zip codes, race, and other such labels are unwarranted. Furthermore, consumers should not be

---

397. Solove & Hartzog, *supra* note 201, at 613-19 (highlighting how the FTC's consent order process "commonly [involves] reporting, audit, and compliance requirements for up to twenty years").

398. *Id.* at 618-19.

399. *Id.* at 614-19 (noting additional consent order measures).

400. The FTC currently must generally rely on a showing of a specific breach of a company's stated privacy practices or violation of the FCRA or ECOA for grounds to bring actions. Furthermore, the FTC does not have sufficient personnel or resources to bring all the necessary enforcement actions. *Id.* at 609, 613. Accordingly, stronger proactive measures are necessary.

401. It is difficult to see how any legitimate economic benefits to the data brokers outweigh the social and communal harms posed by discriminatory use of data.

402. Companies will resist disclosure of rubrics or algorithms that are protected as proprietary information. It will be a challenge to determine when such protection is proper and if there are instances where public values call for overriding such protections.

403. This incentive is similar to that with tax auditing by the IRS. Consumers rationally realize that the IRS does not have resources to audit everyone, but the fear of an audit incentivizes most consumers to comply with tax reporting rules.

rated based on their social connections or familial relations. Companies have access to a vast amount of information that is far more useful in making predictions than such simple assumptions, which are often faulty at best.

Admittedly, it will be very difficult to draw lines. For example, zip codes are sometimes indicative of spending capacity. It is nonetheless more accurate to consider consumers' specific buying histories with a healthy realization that consumers living in a lower-income zip code may have more spending capacity because they are not dumping all of their resources into their homes or apartments. Moreover, zip codes today often include a variety of individuals with a range of incomes and spending behaviors.

In sum, institution of auditing and reporting procedures is necessary to protect consumers' expectations instead of merely relying on industry self-regulation.[404] As other commentators have suggested, the FTC should consider consumer context and varied experiences, and push for bolder data protections that go beyond companies' chosen privacy policies.[405] Moreover, it is essential for regulators to curb the discriminatory use of data that has hidden under the guise of consumer scoring and segmentation.

CONCLUSION

Data brokers track consumers' information and behavior on- and offline, and use this collected data to create consumer segmentations and scores. Companies then secretly use these consumer valuations to determine how they will treat different individuals. Such secret use of consumer data raises significant social and privacy policy concerns within the larger debate about Big Data regulation and how best to protect consumers without overly burdening brokers or restricting data innovations. Indeed, the FTC is studying the data broker industry and has advocated, along with other policymakers, for legislation that requires data brokers to provide greater notice regarding privacy policies and means for opting out of data collection.

While such proposals are a step in the right direction, they do not go far enough in addressing the impact of consumer scoring and segmentation, especially with respect to low-income and other

404. *See* Solove & Hartzog, *supra* note 201, at 625-76.
405. *Id.* at 666-76.

vulnerable consumers. Accordingly, enforcement mechanisms such as ODR systems should support any notice and choice portal for data privacy. Furthermore, strong auditing and reporting requirements should place the burden on data brokers to take reasonable steps to stop and prevent discriminatory use of collected data. The social harms created by scores and classifications that employ discriminatory assumptions outweigh any economic or marketing benefits they arguably provide. This Article thus invites balanced legislation aimed toward protecting consumer "have-nots" in the wake of the Big Data revolution.