# THE PROBLEM OF ONLINE MANIPULATION

*Shaun B. Spencer*[*]

*Recent controversies have led to public outcry over the risks of online manipulation. Leaked Facebook documents discussed how advertisers could target teens when they feel particularly insecure or vulnerable. Cambridge Analytica suggested that its psychographic profiles enabled political campaigns to exploit individual vulnerabilities online. And researchers manipulated the emotions of hundreds of thousands of Facebook users by adjusting the emotional content of their news feeds. This Article attempts to inform the debate over whether and how to regulate online manipulation of consumers. Part II details the history of manipulative marketing practices and considers how innovations in the Digital Age allow marketers to identify, trigger, and exploit individual biases in real time. Part III surveys prior definitions of manipulation and then defines manipulation as an intentional attempt to influence a subject's behavior by exploiting a bias or vulnerability. Part IV considers why online manipulation justifies some form of regulatory response. Part V identifies the significant definitional and constitutional challenges that await any attempt to regulate online manipulation directly. The Article concludes by suggesting that the core objection to online manipulation is not its manipulative nature but its online implementation. Therefore, the Article suggests that, rather than pursuing direct regulation, we add the threat of online manipulation to the existing arguments for comprehensive data protection legislation.*

TABLE OF CONTENTS



[*] Associate Professor, Associate Dean for Academic Affairs, and Director of Legal Skills, University of Massachusetts School of Law–Dartmouth. This work was made possible with the support of the UMass Law Summer Research Grant Program. I am grateful for the thoughtful contributions of Ido Kilovaty and Daniel Susser.

## I. INTRODUCTION

The Digital Age has expanded the tools available to influence people's decisions. Individual-level data are available in real-time, in ever-expanding quantities, about increasingly granular aspects of people's online and real-world behaviors. Fueled by this technological expansion, recent controversies involving potential manipulation of online conduct have drawn public outcry. Leaked Facebook documents discussed how advertisers could target teens online at the times when they feel particularly insecure or vulnerable.[1] Cambridge Analytica suggested that its psychographic profiles enabled political campaigns to exploit individual vulnerabilities online.[2] And researchers manipulated the emotions of

1. Nitasha Tiku, *Get Ready for the Next Big Privacy Backlash Against Facebook*, WIRED (May 21, 2017, 7:00 AM), https://www.wired.com/2017/05/welcome-next-phase-facebook-backlash/.

2. *See, e.g.*, SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 278 (2019) (describing Cambridge Analytica CEO Alexander Nix's claim that Cambridge Analytica's "new analytic methods reveal 'how a customer wants to be sold to, what their personality type is, and which methods of persuasion are most effective[;] . . . [w]hat it does is change people's

hundreds of thousands of Facebook users by adjusting the emotional content of their news feeds.[3]

Stories like these have prompted calls to regulate online manipulation,[4] and leading legal scholars have focused their attention on manipulation. This emerging body of scholarship attempts to define manipulation,[5] considers the circumstances under which manipulation is and is not acceptable,[6] considers why online manipulation is particularly troubling,[7] and offers preliminary thoughts on potential regulatory solutions.[8] This Article attempts to inform the debate over how to address the problem of online manipulation in several ways.[9] First, this Article reviews in depth the history of manipulative marketing practices as well as the increasingly personalized approaches possible as manipulation moves online. Second, this Article identifies the significant definitional and constitutional challenges that would arise in any attempt to regulate manipulation directly. Finally,

behavior through carefully crafted messaging that resonates with them'"); *id.* at 280 (describing former Cambridge Analytica employee Christopher Wylie's claim that the company "exploited Facebook to harvest millions of people's profiles" and "built models to exploit what we knew about them and target their inner demons"). *But see* Elizabeth Gibney, *The Scant Science Behind Cambridge Analytica's Controversial Marketing Techniques*, NATURE (Mar. 29, 2018), https://www.nature.com/articles/d41586-018-03880-4 (noting that "in the real world, it's not clear whether personality-based profiling would be better than the myriad other ways to target people that Facebook already provides"); Jonathan Allen & Jason Abbruzzese, *Cambridge Analytica's Effectiveness Called into Question Despite Alleged Facebook Data Harvesting*, NBC NEWS (Mar. 20, 2018, 2:45 PM), https://www.nbcnews.com/politics/politics-news/cambridge-analytica-s-effectiveness-called-question-despite-alleged-facebook-data-n858256.

3. Adam D. I. Kramer et al., *Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks*, 111 PNAS 8788, 8788 (2014).

4. *See, e.g.*, H.B. No. 2471, 29th Legislature (Haw. 2018) ("[T]he purpose of this Act is to ensure proper oversight of game developers and marketers and protect consumers from predatory and manipulative practices by the gaming industry."); *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us From Exercising Our Right to Privacy*, FORBRUKER RADET 1, 3 (June 27, 2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf (showing "how default settings and dark patterns, techniques and features of interface design meant to manipulate users, are used to nudge users towards privacy intrusive options"); Senator Mark R. Warner, *Potential Policy Proposals for Regulation of Social Media and Technology Firms* 17 (July 2018), https://www.warner.senate.gov/public/_cache/files/d/3/d32c2f17-cc76-4e11-8aa9-897eb3c90d16/65A7C5D983F899DAAE5AA21F57BAD944.social-media-regulation-proposals.pdf (urging regulation of "'dark patterns,' which manipulate user interfaces to steer users towards consenting to settings and practices advantageous to the platform").

5. Susser et al., *Online Manipulation: Hidden Influences in a Digital World*, GEO. L. TECH. REV. (forthcoming 2019) (manuscript 22–23) (https://ssrn.com/abstract=3306006); Cass R. Sunstein, *Fifty Shades of Manipulation*, 1 J. MARKETING BEHAV. 213, 216 (2015).

6. Sunstein, *supra* note 5, at 234; Eric A. Posner, *The Law, Economics, and Psychology of Manipulation*, 12 (U. of Chi. Coase-Sandor Working Paper Series in Law and Economics, Paper No. 726, 2015), http://ssrn.com/abstract=2617481.

7. Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1003–18 (2014); Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRIES L. 157, 171 (2019) [hereinafter Zarsky, *Privacy and Manipulation*] (noting the need to scrutinize digital data-driven practices to determine whether they create a "manipulative imbalance" that requires regulatory or other intervention).

8. Calo, *supra* note 7, at 1041–48; Ido Kilovaty, *Legally Cognizable Manipulation* 34 BERKELEY TECH. L.J. 457, 507 (2019); Zarsky, *Privacy and Manipulation*, *supra* note 7, at 185–86.

9. This Article focuses on manipulation in the commercial context. Online manipulation, of course, is not limited to commercial actors. This Article's discussion of how to define manipulation and the challenges of drafting draft direct regulation of online manipulation may, however, offer insights in other areas. *See infra* Part IV.

this Article suggests that the core problem with online manipulation is not its manipulative nature but its online implementation.

Part II of this Article surveys marketers' past and present practices to exploit consumer biases and vulnerabilities. Part II then considers how future practices may allow marketers to identify or even trigger individual biases and vulnerabilities and then exploit them. Part III surveys proposed definitions of manipulation and identifies the commonalities and points of contention. Part III then defines manipulation as an intentional attempt to influence a subject's behavior by exploiting a bias or vulnerability. Part IV considers why online manipulation is sufficiently troubling to consider some form of regulatory response. The existing infrastructure supporting online behavioral advertising allows for extreme personalization, enabling marketers to identify or even trigger the biases and vulnerabilities that afflict each individual consumer and tailor content to exploit those biases and vulnerabilities. Part V identifies the significant challenges involved in drafting direct regulation of manipulation. Drafting a functional definition to encompass many different biases and vulnerabilities grounded in varied academic disciplines may prove impossible. Causation and harm may be impossible to establish, and direct regulation will undoubtedly draw First Amendment challenges. Finally, the Article concludes by suggesting that the core objection to online manipulation is not its manipulative nature but its online implementation. Online manipulation is just the latest in an escalating series of harms that consumers have faced since the rise of the internet and the establishment of a data-sharing economy. The Article suggests that we use the threat of online manipulation as another argument to support the push for comprehensive data protection legislation.

## II. A HISTORY OF MARKETING AND MANIPULATION

This Part begins by introducing the biases and vulnerabilities that make manipulation possible. Next, this Part describes manipulative techniques that marketers used for decades in the Pre-Digital Era. For the most part, such manipulative techniques allowed "scattershot" appeals to entire markets but could not be tailored to individual consumers.[10] As this Part next describes, however, the explosion of online behavioral advertising in the Digital Age allowed marketers to target manipulative techniques in real time to particular consumers or types of consumers. Finally, this Part considers what will come next by showing how marketers soon could identify, or even trigger or exacerbate, and then exploit the biases and vulnerabilities affecting each individual consumer.

10. *See* Calo, *supra* note 7, at 1014.

### *A. The Biases and Vulnerabilities That Enable Manipulation*

Research in cognitive and social psychology has revealed mechanisms that help explain how people form judgments and make decisions. These mechanisms go by a variety of labels such as intuition,[11] heuristics,[12] biases,[13] and automatic behavior patterns.[14] I refer to these mechanisms collectively as "biases and vulnerabilities." These biases and vulnerabilities help explain why people often make decisions in ways that depart from what an idealized model of rational decision making would predict.[15] That is, they explain why people often make decisions that do not advance their own self-interest.

Marketers are keenly aware of these biases and vulnerabilities. As Jon Hanson and Douglas Kysar observed several decades ago, "consumers . . . are susceptible to manipulation by manufacturers due to their cognitive anomalies. This susceptibility to manipulation produces an opportunity for manipulation that no profit-maximizing manufacturer can ignore."[16] After all, the goal of marketing is "to persuade and manipulate the consumer to enter a deal or to purchase merchandise."[17] They often accomplish this not through argument or debate but by "manipulation of symbols and of our most basic human emotions."[18] Indeed, "the basic premise of the science of marketing is that consumers' purchasing decisions are highly influenced by sellers' manipulation and selling tactics."[19]

The field of behavioral economics has identified many reasons why people exhibit mistaken or ineffective decision making. Daniel Kahneman and Amos Tversky are often acclaimed as founders of behavioral economics.[20] In *Thinking, Fast and Slow*, Kahneman explains the prevailing two-system model of thinking that informs his understanding of how people make decisions.[21] System 1 is a

11. DANIEL KAHNEMAN, THINKING, FAST AND SLOW 4, 10 (2011).

12. *Id.* at 98.

13. *Id.* at 8; Calo, *supra* note 7, at 1002.

14. ROBERT B. CIALDINI, INFLUENCE: THE PSYCHOLOGY OF PERSUASION xiv (rev. ed. 2007) [hereinafter CIALDINI, INFLUENCE]. Cialdini refers to the ways that marketers exploit the psychological principles driving these automatic behavior patterns as "weapons of influence." *Id.* at 1.

15. KAHNEMAN, *supra* note 11, at 411; RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 6–7 (2008). As Hanson & Kysar explain, research in cognitive and behavioral psychology and probability theory revealed "a human decisionmaker model replete with heuristics and biases, unwarranted self-confidence, a notable ineptitude for probability, and a host of other nonrational cognitive features." Jon D. Hanson & Douglas A. Kysar, *Taking Behavioralism Seriously: The Problem of Market Manipulation*, 74 N.Y.U. L. REV. 630, 640 (1999) [hereinafter Hanson & Kysar, *The Problem of Market Manipulation*]. "Consumers are subject to a host of cognitive biases which, particularly when taken together, appear to render them vulnerable to manipulation." *Id.* at 723

16. Hanson & Kysar, *The Problem of Market Manipulation*, *supra* note 15, at 722.

17. Ron Harris & Einat Albin, *Bankruptcy Policy in Light of Manipulation in Credit Advertising*, 7 THEORETICAL INQUIRIES L. 431, 444 (2006).

18. *Id.* at 444 (quoting ANTHONY PRATKANIS & ELLIOT ARONSON, AGE OF PROPAGANDA: THE EVERYDAY USE AND ABUSE OF PERSUASION 5–6 (1991)).

19. Shmuel I. Becher & Yuval Feldman, *Manipulating, Fast and Slow: The Law of Non-Verbal Market Manipulations*, 38 CARDOZO L. REV. 459, 461 (2016).

20. KAHNEMAN, *supra* note 11, at 10; *Not So Smart Now: The Father of Behavioural Economics Considers the Feeble Human Brain*, ECONOMIST (Oct. 29, 2011), https://www.economist.com/books-and-arts/2011/10/29/not-so-smart-now.

21. KAHNEMAN, *supra* note 11, at 20–21; Zarsky, *Privacy and Manipulation*, *supra* note 7, at 170.

fast, automatic, and largely unconscious way of thinking. It is efficient, requires little energy or attention, but is vulnerable to biases and systematic errors.[22] System 2 is a slow, effortful, and controlled way of thinking. It requires energy and attention, but once engaged it can mitigate the vulnerabilities of System 1.[23] As Kahneman explains, the division of labor between the two systems generally works quite well, with System 1 "continuously generating suggestions for System 2: impressions, intuitions, intentions, and feelings," and System 2 mobilized only for situations that System 1 cannot handle.[24] "System 1 has biases, however, systematic errors that it is prone to make in specified circumstances."[25] Manipulators can influence a subject's decision by exploiting cognitive biases that circumvent System 2 and trigger fast action by System 1.[26]

For example, Kahneman explains how one bias, the "anchoring effect," can distort people's estimates.[27] When people first consider a value for an unknown number and then attempt to estimate that number, their estimates will be pulled in the direction of the value that they first considered—even if the value obviously has nothing to do with what they are trying to estimate.[28] In one experiment, Kahneman and Tversky had each subject spin a wheel that was rigged to land on either 10 or 65. They then asked the subject to write down the number and answer two questions: (1) is the percentage of African nations who are UN members higher or lower than the number you wrote; and (2) what is your estimate of the percentage of African nations who are UN members? Although the spin of a wheel obviously has nothing to do with UN membership, subjects who spun a 10 gave average answers of 25%, whereas subjects who spun a 65 gave average estimates of 45%.[29]

The anchoring effect also influences people in real-world settings. In one experiment, real estate agents were asked to assess the value of a house after visiting it and studying a booklet of information about the house, including the asking price.[30] The booklets were identical, with one exception.[31] Half of the agents were shown a high asking price; the other half were shown a low one.[32] Agents who saw the higher asking price gave higher valuations, and vice versa.[33] In fact, the difference between the two groups' averages was 41%.[34] Moreover,

22. KAHNEMAN, *supra* note 11, at 25.

23. *Id.* at 21. Thaler and Sunstein refer to System 1 as the "Automatic System" and System 2 as the "Reflective System." THALER & SUNSTEIN, *supra* note 15, at 19. They describe the Automatic System as your "gut" and the Reflective System as your "conscious thought." *Id.* at 21.

24. KAHNEMAN, *supra* note 11, at 24.

25. *Id.* at 25.

26. Zarsky, *Privacy and Manipulation*, *supra* note 7, at 170. Manipulators can sometimes capitalize on shortcomings in System 2 as well. KAHNEMAN, *supra* note 11, at 34, 119–21 (discussing how System 2 contributes to the anchoring effect by acting as a "lazy controller").

27. KAHNEMAN, *supra* note 11, at 119.

28. *Id.*

29. *Id.*

30. *Id.* at 124.

31. *Id.*

32. *Id.*

33. *Id.*

34. *Id.*

when asked to explain the factors that affected their valuations, they did not list the asking price as a factor.[35] This finding shows that manipulations can be invisible to the user, which makes them all the more powerful as an influence technique.[36]

Similarly, Richard Thaler and Cass Sunstein explain that the availability heuristic affects how people assess the likelihood of future events.[37] Regardless of how likely an event may be, people will judge the event to be more likely if they can easily recall relevant examples.[38] Thus, "[i]n the aftermath of an earthquake, purchases of new earthquake insurance policies rise sharply—but purchases decline steadily from that point, as vivid memories recede."[39]

Other potential sources of manipulation rely on insights from psychology. Robert Cialdini explains how our decisions are driven by what he calls "automatic behavior patterns."[40] Cialdini's extensive field study of sales and marketing professionals identified influence techniques that share several traits.[41] First, they can be activated by a nearly mechanical process.[42] Second, they can be exploited by anyone with knowledge of how to activate them.[43] And third—as is the case with cognitive biases—they work without the subject's awareness.[44] He grouped these influence techniques into six categories: consistency, reciprocation, social proof, authority, liking, and scarcity.[45]

For example, the principle of commitment means that, once we make a commitment, "we will encounter personal and interpersonal pressures to behave consistently with that commitment."[46] Researchers tested this principle by calling a sample of Indiana residents and asking what they would "say if asked to spend three hours collecting money for the American Cancer Society."[47] Many said they would volunteer. A few days later, when researchers called as workers from the American Cancer Society seeking volunteers to collect donations, they

35. *Id.* Kahneman explains that two different mechanisms produce anchoring effects, one from each system. System 2's mechanism is the result of a "weak or lazy System 2," when we consciously try to depart from the anchor, but we stop moving away from the anchor as we become uncertain how far our departure should be. *Id.* at 119–22. System 1's mechanism is its vulnerability to the priming effect, wherein a high anchor evokes an image of a similarly high value for the item you are trying to estimate, and a low anchor evokes an image of a low value. *Id.* at 120, 122.

36. *E.g.*, *id.* at 128 (describing how "your thoughts and behavior may be influenced by stimuli to which you pay no attention at all, and even by stimuli of which you are completely unaware").

37. THALER & SUNSTEIN, *supra* note 15, at 25.

38. *Id.*

39. *Id.*

40. CIALDINI, INFLUENCE, *supra* note 14, at 8.

41. *Id.* at xii–xiii.

42. *Id.* at 11.

43. *Id.*

44. *Id.* "The evidence suggests that the ever-accelerating pace and informational crush of modern life will make this particular form of unthinking compliance more and more prevalent in the future." *Id.* at xiv.

45. *Id.* at xiii.

46. *Id.* at 57.

47. *Id.* at 68.

saw a 700% increase in volunteers.[48] An experiment using a similar methodology significantly increased turnout in a United States presidential election.[49]

Similarly, researchers in California asked homeowners to post a very small sign on their lawns displaying the public service message, "Be a Safe Driver." Later, those homeowners—as well as a control group of other homeowners who were not asked about the earlier sign—were asked to post a large billboard on their lawn reading "Drive Carefully." Only 17% of residents who had not been asked about the lawn sign allowed the billboard, whereas 76% of residents who had committed to the lawn sign also allowed the billboard.[50]

Another influence technique, the principle of social proof, means that we "view behavior as more correct in a given situation to the degree that we see others performing it."[51] For example, the power of social proof emerges in experiments testing whether bystanders will intervene in an emergency. Researchers staged a scene in which smoke seeped under a door. When a single bystander observed the smoke, 75% of the subjects reported the situation. But when a bystander stood with two others who had been instructed to ignore the smoke, only 10% reported the situation.[52] This principle underlies many real world examples, such as bartenders putting money in their own tip jars at the start of the evening; advertisers describing a product as the "fastest-growing" or "largest-selling"; charity drives emphasizing the number of people who have already donated; and nightclub owners creating an unnecessary line at the entrance.[53]

As we shall see in the sections that follow, marketers have exploited subjects' biases and vulnerabilities for decades. The explosion of personalized marketing tools in the Digital Age, however, has made it increasingly possible to identify consumers' vulnerabilities and tailor content to exploit those vulnerabilities.

### *B. Manipulation's Past: The Pre-Digital Era*

This Section describes manipulative marketing techniques in the pre-Digital Age, when personalization was for the most part impossible. Print and broadcast advertisements were aimed at relatively broad audiences. Pricing schemes, terms of service, product packages, and retail environments had to be designed to influence any consumer who came through the door. Direct marketing did allow for some personalization, given the vast stores of consumer profiles that came with the rise of credit reporting agencies and data brokers in the 1950s to

48. *Id.* The 700% increase represents the difference between the percentage of people who volunteered to collect donations without having been called previously (only 4.2%) and the percentage of people who volunteered to collect donations after predicting in a prior call that they would agree (31.1%). Steven J. Sherman, *On the Self-Erasing Nature of Errors of Prediction*, 39 J. PERSONALITY & SOC. PSYCHOL. 211, 217 (1980) (cited in CIALDINI, INFLUENCE, *supra* note 14, at 68).

49. CIALDINI, INFLUENCE, *supra* note 14, at 68.

50. *Id.* at 72.

51. *Id.* at 116.

52. *Id.* at 134–35.

53. *Id.* at 117–18.

the 1970s.[54] Such personalization, however, paled in comparison to the explosion of behavioral data collection and real-time personalization made possible in the Digital Age. Finally, though point-of-sale and door-to-door salespeople could engage in some personalized manipulation, those manipulations rely on one-on-one interactions that do not scale. Thus, marketers could exploit generally applicable biases or vulnerabilities but could not identify or exploit individual consumers' biases or vulnerabilities.

### *1. Print and Broadcast Advertising*

Marketers often find ways to exploit biases and vulnerabilities in the messages they deliver through print and broadcast media. For example, in the investment context, marketers capitalize on the "representativeness heuristic."[55] Individual investors are vulnerable to the mistaken assumption that past investment performance predicts performance.[56] Financial firms capitalize on this bias by featuring their past performance in their marketing materials.[57] Although the firms avoid potential regulatory backlash by including disclaimers to the effect that "past performance does not guarantee future results," individual investors are more likely to pay attention to the past performance evidence than the disclaimer.[58]

Marketers also exploit the availability heuristic "by simply maximizing the frequency and intensity of advertisements."[59] "[T]he human desire to observe patterns in random events . . . might be utilized by manufacturers to generate false images of what behavior or characteristics are representative of users of a product."[60] For example, consumers considering investment vehicles tend to place too much weight on product attributes that appeared in advertisements.[61] Relying on these attributes leads investors to make decisions that depart from

54. AARON RIEKE ET AL., OPEN SOCIETY FOUNDATION, DATA BROKERS IN AN OPEN SOCIETY 5–6 (2016), https://www.opensocietyfoundations.org/sites/default/files/data-brokers-in-an-open-society-20161121.pdf (noting that credit bureaus begin in the 1950s as "small, local data brokers that arose to help provide lenders with better information about prospective borrowers[,]" and that the modern practice of segmenting consumers for marketing purposes began in the 1970s); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 9 (2014) (describing the rise of Fair, Isaac & Co. in the 1950s to become the first credit reporting agency, eventually knows as FICO).

55. Ramzi Boussaidi, *Representativeness Heuristic, Investor Sentiment and Overreaction to Accounting Earnings: The Case of the Tunisian Stock Market*, 81 PROCEDIA SOC. & BEHAV. SCI. 9, 10 (2013), https://doi.org/10.1016/j.sbspro.2013.06.380 ("In the stock markets, an investor subject to the representativeness heuristic interprets the past performance of firms as being representative of a general performance that the firm will continue to generate in the future.").

56. Martin Brenncke, *The Legal Framework for Financial Advertising: Curbing Behavioural Exploitation*, 19 EUR. BUS. ORG. L. REV. 853, 857–58 (2018) (citing Alan R. Parmiter & Ahmed E. Taha, *Mutual Fund Performance Advertising: Inherently and Materially Misleading?*, 46 GA. L. REV. 292 (2012)), https://doi.org/10.1007/s40804-018-0111-9.

57. *Id.* at 860.

58. *Id.* at 875.

59. Hanson & Kysar, *The Problem of Market Manipulation*, *supra* note 15, at 731.

60. *Id.*

61. Brenncke, *supra* note 56, at 858.

traditional economic models.[62] Thus, the "availability heuristic can explain why retail investors base their investment decisions on sales material that is readily available and presented in prominent style without entering into a deep search for information."[63]

Advertisements can also exploit the "irrelevant third option effect" to influence consumer decisions.[64] Introducing irrelevant options typically biases a consumer in favor of options that the consumer originally disfavored.[65] For example, after widespread publicity about the harmful effects of ephedra in diet pills, some dietary supplement manufacturers marketed their products as "ephedra free."[66] Despite the fact that none of the supplements in question had ever contained ephedra, the suggestion of a nonexistent "ephedra option" led consumers to perceive the "ephedra free" supplements as less risky.[67]

### *2. Pricing and Terms of Service*

Marketers also rely on influence techniques that do not depend on traditional advertising. Instead, these techniques influence consumers through the way that they structure their pricing and terms of service. For example, one of the most common phenomena that marketers exploit when pricing their products is "price blindness." By pricing products with a nine in the right most digit—*e.g.*, $1.99 rather than $2.00 or $19,999 rather than $20,000—marketers induce consumers to view the slightly lower price as significantly different from the rounded-up price.[68]

When deciding what pricing options to offer across a product line, manufacturers can influence consumer preferences by introducing an irrelevant option which they expect consumers to reject, in order to enhance the attractiveness of the real option. For example, "manufacturers can make products appear less expensive by adding a higher-priced option to the product line."[69] For the same reason, used car salespeople prefer not to show prospective buyers just one car. Instead, they introduce irrelevant options to bias the consumer in favor of options she may originally have disfavored.[70]

62. *Id.* at 858–59.

63. *Id.* (citing Ruben Cox & Peter de Goeij, What Do Investors Learn from Advertisements? (Sept. 8, 2017) (unpublished manuscript) https://ssrn.com/abstract=3034144).

64. Jon D. Hanson & Douglas A. Kysar, *Taking Behavioralism Seriously: Some Evidence of Market Manipulation*, 112 HARV. L. REV. 1420, 1515 (1999) [hereinafter Hanson & Kysar, *Some Evidence of Market Manipulation*].

65. Michael A. McCann, *Dietary Supplement Labeling: Cognitive Biases, Market Manipulation & Consumer Choice*, 31 AM. J.L. & MED. 215, 224 (2005) (citing Hanson & Kysar, *Some Evidence of Market Manipulation*, *supra* note 64, at 1440) (noting the effect with used car sales).

66. Michael A. McCann, *Dietary Supplement Labeling: Cognitive Biases, Market Manipulation & Consumer Choice*, 31 AM. J. L. & MED. 215, 224 (2005).

67. *Id.*

68. *See generally* Hanson & Kysar, *Some Evidence of Market Manipulation*, *supra* note 64, at 1442–43.

69. Hanson & Kysar, *The Problem of Market Manipulation*, *supra* note 15, at 734.

70. Hanson & Kysar, *Some Evidence of Market Manipulation*, *supra* note 64, at 1440.

Marketers also exploit the anchoring effect in retail pricing. Car dealers, for example, trade on this effect by placing a high sticker price on each car.[71] Similarly, supermarkets can use the anchoring effect to increase the amount of products people buy. One supermarket, for example, varied the signage that it used to promote Campbell's soup. On some days, the signage read, "Limit of 12 per person," while on other days it read, "No limit per person." The price did not change, but consumers bought twice as many cans of Campbell's soup (an average of seven cans) when the signage referenced the twelve can limit.[72]

Terms of service can also exploit consumer biases and vulnerabilities. For example, marketers capitalize on the "endowment effect" by getting their products into the hands of the consumer through "money-back guarantees, test drives, thirty-day no-risk trial periods, free samples, and other marketing ploys, all of which are designed to create in the consumer a sense of ownership."[73] The endowment effect may lead the consumer to place a higher value on the product, but because people are unaware that the effect will influence their judgment, consumers do not see the "risks" of taking the product home.[74] Marketers can also exploit the status quo bias, which Sunstein and Thaler describe as "people's tendency to stick with their current situation."[75] Marketers often exploit this bias by offering free trial subscriptions that automatically renew unless consumers cancel them.[76]

Similarly, framing effects can influence whether consumers experience a transaction as a loss or a gain. This framing is important because people tend to value a loss as less desirable than an equivalent gain is desirable.[77] Thaler describes how credit card companies pressured American retailers to frame

> any difference between [prices for] cash and credit card customers . . . [in] the form of a cash discount rather than a credit card surcharge. This preference makes sense if consumers would view the cash discount as an opportunity cost of using the credit card but the surcharge as an out-of-pocket cost.[78]

Thus, framing the price differential as a cash discount predisposed consumers to view the difference as a gain due to using cash, rather than a loss due to using a credit card.[79]

71. *Id.*
72. KAHNEMAN, *supra* note 11, at 126.
73. Hanson & Kysar, *The Problem of Market Manipulation*, *supra* note 15, at 734.
74. *Id.*
75. THALER & SUNSTEIN, *supra* note 15, at 34.
76. *Id.* at 35.
77. Richard A. Thaler, *Toward a Positive Theory of Consumer Choice*, J. ECON. BEHAV. & ORG. 39, 42 (1980).
78. *Id.* at 45.
79. *Id.*

### *3. Product Labeling and Retail Environment*

Marketers also use product labeling and the retail store environment to influence consumer decisions. For example, marketers rely on the framing effect when they label a food as "75% lean" rather than "25% fat." Although both are accurate, consumers are more favorably disposed to the positive framing of the product as "lean."[80]

Marketers also manipulate consumer perceptions by altering product packaging based on the "just noticeable difference" phenomenon.[81] "[H]umans exhibit various thresholds of awareness such that a certain degree of change in a sensory stimulus is required before the change becomes noticeable to observers."[82] Marketers use these thresholds "to implement hidden price increases: 'In order to keep the price of a product fairly stable manufacturers will often decrease its size, in increments carefully calibrated to be less than the consumer's [just noticeable difference].'"[83] For example, a 1991 New York Attorney General investigation found dozens of these size reductions, such as Rice-a-Roni reduced from 8 to 6.8 ounces and chocolate milk reduced from 16 to 14.5 ounces, all without any change in price or package appearance.[84]

Additionally, researchers find that consumers' shopping habits are affected by their mood, and that consumers in positive moods pay less attention to marketing messages and rely more on heuristics.[85] Inducing the proper mood, therefore, can help marketers capitalize on the "nonrational, experiential mode of information processing that consumers utilize when in affective response modes."[86]

For example, marketers use the retail environment to maximize unplanned purchases by piping in aromas to increase bakery sales, arranging deli sections to "create the illusion of choice," and manipulating the lighting, aisle width, heating, or color schemes.[87] Similarly, marketers place popular staples at opposite ends of the grocery store to force customers to cover the maximum amount of ground; design produce sections as mazes to encourage wandering; place high-end products in wider aisles to encourage browsing; place children's brands on lower shelves to induce children to grab them on their own; and stock soup cans

80. Hanson & Kysar, *Some Evidence of Market Manipulation*, *supra* note 64, at 1451; Irwin P. Levin & Gary J. Gaeth, *How Consumers Are Affected by the Frame of Attribute Information Before and After Consuming the Product*, 15 J. CONSUMER RES. 374, 374 (1988).

81. Hanson & Kysar, *Some Evidence of Market Manipulation, supra* note 64, at 1449.

82. *Id.*

83. *Id.* (quoting DAVID A. STATT, UNDERSTANDING THE CONSUMER: A PSYCHOLOGICAL APPROACH 45 (1997)).

84. *Id.* at 1449 n.139 (citing Martin Sloane, *Reducing Product Sizes Is a Growing Practice*, HOUS. CHRON., May 22, 1991, at 4).

85. *Id.* at 1444–45 (citing MICHAEL R. SOLOMON, CONSUMER BEHAVIOR: BUYING, HAVING & BEING 313 (4th ed. 1999)).

86. *Id.* at 1445.

87. *Id.* at 1445–46.

out of alphabetical order to force customers to search through many types of cans.[88]

Retailers also know that warm colors increase arousal and excitement, whereas cool colors increase relaxation and enhance browsing and purchasing behaviors. Therefore, retailers use "warm colors on store windows and entrances to attract customers physically into the store, and then utilize cool colors in displays."[89] For similar reasons, retailers also vary the color in which they present prices based on the likely consumer's gender. Male customers perceive greater savings when prices are presented in red, whereas female customers perceive greater savings when prices are presented in black.[90]

Restaurants tailor the environment to influence consumers as well. Many restaurants play slow rather than fast background music because the slower music encourages patrons to stay longer and make more purchases.[91] Fast-food restaurants, however, play faster music to encourage faster turnover.[92]

### *4. Direct Sales*

The pre-Digital Age marketing medium that allowed for the most personalization was direct sales contact, whether at the marketer's retail site or through door-to-door sales. Salespeople have long structured these interactions to manipulate consumers.

Clothing store salespeople exploit what Cialdini calls the "contrast principle" by making sure to sell customers the most expensive product they are interested in first.[93] For example, if a customer wanted to look at both a suit and a sweater, the salesperson would sell the suit first.[94] Because the customer already encountered the more expensive suit, the customer will find the sweater to be even less expensive than if the customer had considered the sweater in the first place.[95] In contrast, selling the suit after the sweater would cause the customer to perceive the suit as even more expensive.[96] In fact, a customer who enters a clothing store to buy a suit "will almost always *pay more* for whatever accessories he buys if he buys them after the suit purchase than before."[97] Similarly, automobile dealers use the contrast principle by first concluding the negotiation on the price of a new car before moving on to discuss additional options and accessories.[98] After committing to the high cost of the car, the cost of various options, accessories, and extended warranties seems almost trivial.[99]

88. *Id.* at 1447–49.
89. Becher & Feldman, *supra* note 19, at 477–78.
90. *Id.* at 478.
91. *Id.* at 479.
92. *Id.*
93. CIALDINI, INFLUENCE, *supra* note 14, at 13.
94. *Id.*
95. *Id.*
96. *Id.*
97. *Id.*
98. *Id.* at 14.
99. *Id.*

In-home salespeople can exploit vulnerabilities as well. For example, a successful home fire alarm salesperson relied on the principle of trust to prompt prospective customers to buy his products.[100] During his home visits, the salesperson would say that he forgot a book in his car and ask if he could let himself out and back in while the prospects were completing some paperwork.[101] People always complied, often by giving him the key. The salesperson did this because people would only allow someone they trusted to let themselves back in, and he wanted to be associated with trust.[102]

As Calo recognizes, real-world salespeople can get a sense of their customer based on cues from their behavior, clothing, or accessories, and then tailor their presentation accordingly.[103] In fact, a salesperson may even detect a bias or vulnerability in the customer and exploit it.[104] These techniques, however, rely on direct, one-to-one interactions, and therefore cannot scale in the way that digital marketing techniques can. The next Section examines how the explosion of data collection, analysis, and use in the Digital Age's enhances marketers' ability to manipulate consumers.

### *C. Manipulation's Present: The Digital Era*

The emergence of the internet allowed marketers to target individuals in real time based on increasingly granular data about their online and real-world behaviors.[105] Internet marketing began in the mid-1990s with the launch of the World Wide Web.[106] It started with banner advertisements that advertisers could deliver to whoever visited particular websites.[107] These banner ads were an early example of "contextual advertising"—ads based on a single website visit or search query "without the collection and retention of data about the consumer's online activities over time."[108] When based upon the likely interests of website viewers, contextual advertising is roughly analogous to pre-Digital Age print or broadcast advertising based on the expected audience. Advertising based on a

100. ROBERT CIALDINI, PRE-SUASION: A REVOLUTIONARY WAY TO INFLUENCE AND PERSUADE 6–7 (2016) [hereinafter CIALDINI, PRE-SUASION].

101. *Id.* at 7.

102. *Id.*

103. Calo, *supra* note 7, at 1021.

104. *Id.*

105. In the pre-Internet age, marketing was still data driven, and data brokers collected vast amounts of data. Concerns about the volume, sensitivity, and irrelevance of the data they collected and used for credit assessment purposes led to passage of the Fair Credit Reporting Act of 1970. The rise of the Digital Age, however, has dramatically expanded not only the volume of data collected about consumers, but also the variety and granularity of data collected and the ease with which the data may be collected, analyzed, and then used to make decisions and predictions in real time. *See* Chris Jay Hoofnagle, Essay Prepared for the Future of Privacy Forum's Big Data and Privacy: Making Ends Meet Event: How the Fair Credit Reporting Act Regulates Big Data (Sept. 10, 2013), https://fpf.org/wp-content/uploads/LEGAL-Hoofnagle-How-FCRA-Regulates-Big-Data.pdf.

106. Peter S. Menell, *Regulating "Spyware": The Limitations of State "Laboratories" and the Case for Federal Preemption of State Unfair Competition Laws*, 20 BERKELEY TECH. L.J. 1363, 1395 (2005).

107. *Id.*

108. FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 30 (2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.

subject's search query, of course, is more particularized than advertising based on an expected website's audience. Nevertheless, contextual advertising does not rely on a profile built over time.[109]

In contrast, online behavioral advertising involves building a profile of a subject's online behaviors in order to deliver highly individualized advertising.[110] To accomplish online behavioral advertising, merchants must track each consumer's "online activities over time—including the searches the consumer has conducted, the web pages visited, and the content viewed—in order to deliver advertising targeted to the individual consumer's interests."[111] Online behavioral advertising technology allowed merchants to perform behavioral targeting "based on 'prior search queries, prior search results, [and] demographic, geographic, psychographic and activity information.'"[112] "First party" online behavioral advertising relies only upon the information collected by a single company.[113] In contrast, "third party" online behavioral advertising dramatically expands the scope of profiling by enlisting advertising networks that aggregate behavioral data across many participating websites.[114] And online behavioral profiling tracks consumers as they access online games, social media, and other apps through their mobile devices, which permits far more granular behavioral data collection, including location-based tracking.[115] In addition, behavioral advertising's constantly increasing capabilities enable the emergence of "psychographic" techniques that link "objective demographic characteristics—age, gender, and Internet use—with more abstract characteristics like peer group interests, ideas, and opinions" and use the resulting profile to determine what particular groups are likely to buy.[116]

Calo captures the degree to which Digital Age marketers can influence consumers in his description of the "mediated consumer."[117] Calo explains that technology "mediates a consumer's interactions with the market," which allows marketers to record detailed information about the consumer's online interactions and allows marketers to "design every aspect of the interaction with the consumer."[118] This control extends to both the "physical and virtual interface where

109. *Id.*
110. *See id.*
111. *Id.* at 46 (emphasis omitted).
112. Steven C. Bennett, *Regulating Online Behavioral Advertising*, 44 J. MARSHALL L. REV. 899, 901 (2011) (alteration in original) (quoting Loren Baker, *Google Advertising Patents for Behavioral Targeting, Personalization and Profiling*, SEARCH ENGINE J. (Oct. 7, 2005), http://www.searchenginejournal.com/google-advertising-patents-for-behavioral-targeting-personalization-and-profiling/2311/).
113. *Id.*
114. *Id.* at 901–02; *see* FED. TRADE COMM'N, *supra* note 108, at 2–3.
115. Bennett, *supra* note 112, at 903–04.
116. *Id.* at 904.
117. Calo, *supra* note 7, at 1003.
118. *Id.* at 1003–04.

the interaction occurs."[119] As the examples below illustrate, that degree of control over the customer experience enhances Digital Age marketers' ability to exploit consumer biases and vulnerabilities.[120]

The European Commission recently studied the extent to which EU marketers attempt to "exploit behavioral drivers of vulnerability."[121] For example, some marketers engaged in "drip pricing" by showing consumers only part of the price up front, "with additional costs and charges being shown at later stages."[122] The practice is especially prevalent in e-commerce involving airline tickets, mobile phone contracts, and hotel bookings.[123] Drip pricing exploits the commitment principle, which pressures consumers to make subsequent decisions that are consistent with decisions they have already made.[124]

The European Commission found several other practices that exploited consumer biases and vulnerabilities. For example, marketers exploit the scarcity principle by using limited-time offers and using "dynamic pricing" to change the price of goods and services depending on the circumstances.[125] They also exploit the social proof principle[126] by indicating how many other consumers are considering the same offer.[127] And they exploit the "decoy effect"[128] by engaging in "reference pricing," which means "showing the price of a product alongside a different price ('older' price or price of a competing product)."[129] Furthermore, marketers exploit the commitment principle[130] by "baiting," *i.e.*, "advertising a limited number of a very limited number of discounted products or services, with an expectation that a consumer will purchase a non-discounted product once the discounted one is no longer available."[131] The European Commission noted that this was common in the finance sector's use of teaser rates.[132] Finally, the European Commission's report noted that marketers "exploit consumers' limited capacity to process complex information."[133] They present information "in ways

119. *Id.* at 1004.

120. *See* Eliza Mik, *The Erosion of Autonomy in Online Consumer Transactions*, LAW, INNOVATION & TECH., 4-2016, at 1, 2 ("In the context of business-to-consumer online commerce, technology augments the decision-making capabilities of businesses and enables them to exert more influence over consumer choices than in traditional transactional settings.").

121. *European Commission*, *Consumer Vulnerability Across Key Markets in the European Union: Final Report*, at 308 (Jan. 2016), https://ec.europa.eu/info/sites/info/files/consumers-approved-report_en.pdf.

122. *Id.* at 310.

123. *Id.*

124. *See* CIALDINI, INFLUENCE, *supra* note 14, at 67.

125. *European Commission*, *supra* note 121, at 310.

126. CIALDINI, INFLUENCE, *supra* note 14, at 116.

127. *European Commission*, *supra* note 121, at 310.

128. DAN ARIELY, PREDICTABLY IRRATIONAL: THE HIDDEN FORCES THAT SHAPE OUR DECISIONS 10 (rev. ed. 2009); Jerel E. Slaughter, et al., *The Decoy Effect as a Covert Influence Tactic*, 24 J. BEHAV. DECISION MAKING 249, 250 (2011), https://www.researchgate.net/publication/236028106_The_Decoy_Effect_as_a_Covert_Influence_Tactic ("The decoy effect occurs when the addition of an inferior candidate to a choice set changes the preference relations among the existing, superior alternatives . . . .").

129. *European Commission*, *supra* note 121, at 310.

130. CIALDINI, INFLUENCE, *supra* note 14, at 36–37.

131. *European Commission*, *supra* note 121, at 311 (citation omitted).

132. *Id.*

133. *Id.*

that make it difficult for consumers to understand the true cost of products or services they are purchasing[,]" whether through bundling multiple products or services together or creating complex financial products.[134]

One team of researchers demonstrated that they could use the social proof[135] principle to increase voter turnout. Bond et al. tested whether they could influence voter turnout by manipulating messages in subjects' Facebook news feeds.[136] They conducted a randomized control trial of the 61 million Facebook users age eighteen and older who accessed Facebook on the day of the 2010 Congressional midterm elections.[137] They randomly assigned subjects to three groups. The "informational message" group saw a message that encouraged them to vote, offered a link to polling place information, contained a clickable "I voted" button, and showed a counter of how many other Facebook users had voted.[138] The "social message" group saw the same message but also saw six randomly selected profile pictures of the subject's Facebook friends who had already voted.[139] The control group received no message.[140] The researchers then determined the subjects' voting status by examining public voting records.[141] Users who received the social message were 0.39% more likely to vote than users who received the informational message and users who received no message at all.[142] Users who saw the informational message were no more likely to vote than those who received no message at all, which strongly suggests that subjects were vulnerable to the "social proof" aspect of the message.[143]

Facebook offered a vivid preview of personalized Digital Age manipulation in documents leaked to an Australian newspaper.[144] Documents prepared for a potential advertiser showed that Facebook "had offered advertisers the opportunity to target 6.4 million younger users, some only 14 years old, during moments of psychological vulnerability, such as when they felt 'worthless,' 'insecure,' 'stressed,' 'defeated,' 'anxious,' and like a 'failure.'"[145] The document emphasized that Facebook could micro-target ads at the "moments when young people need a confidence boost."[146] The document also showed that Facebook monitored "posts, photos, interactions, and internet activity in real time to track

134. *Id.*

135. CIALDINI, INFLUENCE, *supra* note 14, at 116.

136. Robert M. Bond et al., *A 61-Million-Person Experiment in Social Influence and Political Mobilization*, 489 NATURE 295, 295 (2012).

137. *Id.*

138. *Id.*

139. *Id.*

140. *Id.*

141. *Id.*

142. *Id.* at 295–96. That percentage (0.39%) may seem quite small, but the scale of the experiment had a substantial effect. The researchers estimated that their "social message" intervention led to 60,000 additional votes in the 2010 midterm elections, plus another 280,000 who voted as a result of a "social contagion" effect. ZUBOFF, *supra* note 2, at 300.

143. Bond et al., *supra* note 136, at 296.

144. Tiku, *supra* note 1.

145. *Id.*

146. *Id.*

these emotional lows."[147] One professor of public relations and social media called this type of targeting the "holy grail of advertising," and explained that the return on investment is "huge" when marketers can target their messages to exactly what consumers are feeling at a given moment.[148]

Additionally, online platforms can exploit consumer vulnerabilities to influence the extent to which consumers protect their own privacy.[149] For example, the endowment effect leads consumers to "value privacy more if they already have it than if they must acquire it,"[150] so setting privacy-minimizing default options will bias consumers toward undervaluing privacy. In fact, data from 2012 show how personal disclosure on Facebook "was trending fairly sharply downward until, around 2009, the company changed some of its privacy defaults," at which point disclosure "began steadily to climb again."[151] Similarly, Keith et al. have documented a phenomenon they call "privacy fatigue," meaning "the tendency of consumers to disclose greater information over time when using more complex and less-usable privacy controls."[152] The researchers found that online marketers could "create complex controls that both excite consumers initially yet also encourage excessive information disclosure over time because of the inherent tradeoff in usability."[153] This phenomenon acts as a "trap" for consumers because more complex privacy tools give consumers a perception of greater ease of use, yet in fact lead to more disclosure.[154]

Finally, with the rise of big data and sophisticated analytics, merchants need not set out to exploit particular biases or vulnerabilities. Instead, they can use A/B testing to experiment with various versions of marketing materials and messages until they find the versions that best exploit consumers' vulnerabilities.[155] Leading online platforms and marketers use A/B testing to improve

147. *Id.*

148. *Id.* Calo cites a similarly disconcerting study "purport[ing] to show that women feel less attractive on Monday mornings. Based on its findings, the study recommended that companies concentrate on these 'prime vulnerability moments' to sell beauty products." Calo, *supra* note 7, at 996 (citing Rebecca J. Rosen, *Is This the Grossest Advertising Strategy of All Time?*, ATLANTIC, (Oct. 3, 2013, 1:46 PM), http://www.theatlantic.com/technology/archive/2013/10/is-this-the-grossest-advertising-strategy-of-all-time/280242). Although this study identifies an across-the-board vulnerability, one could take an approach similar to that identified in the Australian Facebook leak to identify when users feel least attractive and then target them with manipulative advertisements.

149. Although these interactions may not be traditional "marketing" in the sense of persuading a consumer to buy a product, the practices merit mention here because the platforms are financially dependent on monetizing users' personal data.

150. Calo, *supra* note 7, at 1013.

151. *Id.* at 1013 n.103 (citing Fred Stutzman et al., *Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, 4 J. PRIVACY & CONFIDENTIALITY, no. 2, 2012, at 7, 17).

152. MARK J. KEITH ET AL., PRIVACY FATIGUE: THE EFFECT OF PRIVACY CONTROL COMPLEXITY ON CONSUMER ELECTRONIC INFORMATION DISCLOSURE 2 (2014).

153. *Id.*

154. *Id.* at 14.

155. Calo, *supra* note 7, at 1010; Ron Kohavi & Stefan Thomke, *The Surprising Power of Online Experiments*, HARV. BUS. REV., Sept.–Oct. 2017, https://hbr.org/2017/09/the-surprising-power-of-online-experiments ("In an A/B test the experimenter sets up two experiences: 'A,' the control, is usually the current system and considered the "champion," and 'B,' the treatment, is a modification that attempts to improve something—the 'challenger.' Users are randomly assigned to the experiences, and key metrics are computed and compared.").

nearly any aspect of their online presence such as website features, user interfaces, product recommendation algorithms, and shipping terms.[156] Marketers using A/B testing could effectively stumble into manipulative tools as a result of such experimentation, rather than intentionally developing tools to exploit a known bias or vulnerability.[157]

### *D. Manipulation's Future: The Potential for Individualized Manipulation in the Evolving Digital Age*

The prior two sections considered how past and present marketing techniques could exploit consumers' biases and vulnerabilities. This Section considers the possibility that, in the near future, marketers could expand upon these techniques by exploiting or even triggering biases and vulnerabilities at the individual consumer level, rather than relying on biases and vulnerabilities prevalent in the general population. This Section also assesses how close marketers are to making that potential a reality and concludes that they are quite close.

As Calo observes, online behavioral advertising today generally matches ads to users in real time based on an assessment of how relevant the ads are to the user.[158]

> The bulk of the tracking that one reads about goes to determining the likely preferences of a given consumer so as to show her the product or service, the ad for which is already in inventory, that seems most likely to resonate. In other words, the "behavioral" in behavioral tracking refers to the previous behavior of the user online, which then serves to sort that user into a particular category for ad-matching purposes.[159]

Online marketers, however, are poised to do much more than predict relevant ads.[160]

While everyone has cognitive biases, "not everyone has the *same* biases or experiences them to the same degree."[161] Therefore, marketers would find it extremely valuable to tailor their marketing messages to best exploit the biases and vulnerabilities of each individual consumer. If successful, such an approach would significantly increase their marketing success, just as predictive analytics increased marketing success rates by allowing marketers to target consumers more likely to buy their products.[162]

Marketers could use the existing infrastructure of online behavioral advertising to exploit individual biases and vulnerabilities in several ways. First, they

156. Kohavi & Thomke, *supra* note 155.

157. Calo, *supra* note 7, at 1010; Zarsky, *Privacy and Manipulation*, *supra* note 7, at 170.

158. Calo, *supra* note 7, at 1016.

159. *Id.*

160. *Id.*

161. *Id.* at 1014 (citing Lester K. John et al., *Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information*, 37 J. CONSUMER RESEARCH 858, 863-68 (2011)).

162. Shaun B. Spencer, *Privacy and Predictive Analytics in E-Commerce*, 49 NEW ENG. L. REV. 629, 635 (2015) ("Predictive analytics can make online behavioral advertising more efficient by showing ads to consumers who are more likely to click on them.").

could discover an individual consumer's vulnerabilities and then tailor their marketing materials or web architecture in real time to exploit those biases and vulnerabilities.[163] Second, marketers could trigger or exacerbate particular individuals' vulnerabilities before exploiting them. This Section considers how close marketers currently are to using each of these techniques.

### *1. Identifying and Exploiting Individual Biases and Vulnerabilities*

The steps necessary to identify and exploit individual biases and vulnerabilities are quite similar to the existing approach to online behavioral advertising. First, marketers would need to link particular behavioral profiles to particular biases or vulnerabilities. Second, marketers would need to identify consumers who exhibit those profiles. Finally, marketers would need to target each consumer an intervention crafted to exploit the corresponding bias or vulnerability.

#### a. Identifying Individual Biases and Vulnerabilities in Real Time

The current approach to online behavioral advertising shows that marketers can already make real-time assessments of a subject's interests based on the subject's behavioral profile. The next step toward exploiting individual biases and vulnerabilities would be to use that same behavioral profile to determine the subject's biases or vulnerabilities.

Calo summarized several research areas that support such an approach.[164] One emerging area of research called "persuasion profiling" begins from the premise that "consumers differ in their susceptibility to various forms of persuasion."[165] Persuasion profiling allows companies to "discover what motivates a given consumer and dynamically change the advertisement accordingly in real time."[166] Calo points out a second research field which recognizes "that consumers have different 'cognitive styles,' or ways of thinking and engaging with the world."[167] Researchers are developing "ways to test the subject's cognitive style and then dynamically alter the layout of the test website accordingly—a technique they label 'morphing.'"[168]

Though these fields are still emerging, researchers and marketers have already demonstrated ways to use online behavioral profiling to identify biases and vulnerabilities.[169] For example, researchers have predicted the "big five" personality traits based on mobile phone logs and contact data.[170] Researchers have also

163. Calo, *supra* note 7, at 1010. ("Trouble arises when firms start looking at the consumer behavior dataset to identify consumer vulnerabilities.").

164. *Id.* at 1032.

165. *Id.* at 1017.

166. *Id.*

167. *Id.* (citing such differences as impulsive versus deliberative or visual versus reader).

168. *Id.*

169. *See infra* text accompanying notes 170–71.

170. Yves-Alexandre de Montjoye et al., Predicting Personality Using Novel Mobile Phone-Based Metrics, *in* LECTURE NOTES IN COMPUTER SCI.: 6TH INT'L. CONF. ON SOC. COMPUTING, BEHAV. CULTURAL MODELING, AND PREDICTION (2013).

used social network profiles to predict traits such as impulsivity, depression, sensationalist interest, life satisfaction, emotional stability, drug use, sexual orientation, and political views.[171]

Amazon, Google, and IBM have filed patent applications concerning the use of smart speakers and other devices to detect subjects' moods, a process referred to as "dynamic emotional targeting."[172] Amazon's patent suggested that its smart speaker Alexa could analyze the pitch and volume of user's commands to determine the subjects' moods, and "respond to commands accordingly, maybe with 'highly targeted audio content, such as audio advertisements or promotions.'"[173] Google has also filed a patent "for a method to augment devices to detect negative emotions; the devices will then automatically offer advice."[174] And IBM has filed a patent for a process that helps search engines "return web results based on the user's 'current emotional state,'" based on indicia of mood drawn from webcam facial recognition, a scan of the user's heart rate, and even the "user's brain waves."[175]

Similarly, researchers have used keyboard typing patterns to predict emotional states such as confidence, nervousness, sadness, and tiredness.[176] More broadly, mobile phone sensor data could be used to predict mood, personality, stress levels, gender, marital and job status, age, level of disease, mental health issues, sleep, and physical movement.[177]

Facebook has developed an algorithm that scans and analyzes social media activity for "indications of immediate suicide risk."[178] The algorithm scans the "posts, comments and videos of users in the United States and other countries."[179] If the algorithm finds significant indicia of suicide risk, it flags for a Facebook employees who then considers whether to refer the activity to local law enforcement.[180]

Finally, Calo cites psychological research "suggesting that willpower is a finite resource that can be depleted or replenished throughout the day."[181] He proposes that advertisers could simply count how many decisions a subject had

171. Wu Youyou et al., *Computer-Based Personality Judgments Are More Accurate Than Those Made by Humans*, 112 PNAS 1036, 1038 (2015).

172. Sidney Fussell, *Alexa Wants to Know How You're Feeling Today*, THE ATLANTIC (Oct. 12, 2018), https://www.theatlantic.com/technology/archive/2018/10/alexa-emotion-detection-ai-surveillance/572884/.

173. *Id.*

174. *Id.*

175. *Id.*

176. Clayton Epp et al., Identifying Emotional States Using Keystroke Dynamics*, in* PROC. OF THE SIGCHI CONF. ON HUM. FACTORS IN COMPUTING SYSTEMS 715 (2011), http://hci.usask.ca/uploads/203-p715-epp.pdf.

177. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (2015); Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 115–16 (2014).

178. Natasha Singer, *In Screening for Suicide Risk, Facebook Takes on Tricky Public Health Role*, N.Y. TIMES (Dec. 31, 2018), https://www.nytimes.com/2018/12/31/technology/facebook-suicide-screening-algorithm.html.

179. *Id.*

180. *Id.*

181. Cato, *supra* note 7, at 996 (citing Roy F. Baumeister & John Tierney, WILLPOWER: REDISCOVERING THE GREATEST HUMAN STRENGTH 1–5 (2011)).

made already, which would allow them to infer when the user's willpower was depleted.[182]

b. Exploiting Individual Biases and Vulnerabilities in Real Time

As shown above, marketers can already identify some individual biases and vulnerabilities in real time, and the emerging research suggests that they will rapidly expand their ability to do so.[183] In addition, marketers have already proven with online behavioral advertising that they can target different advertisements, offers, and terms of service in real time,[184] and they can already use marketing messages, pricing, terms of service, and web design to exploit vulnerabilities found in the general population.[185] There seems little doubt that marketers will develop the ability to exploit individual biases and vulnerabilities as they are identified in real time. In fact, a team of researchers has already done so.

Matz et al. put this approach into practice on Facebook.[186] They conducted three experiments designed to test whether they could accomplish what they called "psychological persuasion" online, in real time, across a high volume of users.[187] Using Facebook data, they tested whether tailoring advertisements to appeal to individual users' personality traits would increase advertising effectiveness.[188] Facebook did not sell or share any of these users' data with the researchers. Instead, the researchers used Facebook's "Facebook Likes" feature to serve their ads to users who exhibited the desired patterns of likes.[189] They determined which patterns to target by using a database (myPersonality.org) that blended millions of users' Facebook Likes with their scores on an International Personality Item Pool ("IPIP") questionnaire, a "widely validated and used personality measure."[190] The researchers then selected ten likes that demonstrated the highest and lowest scores for two personality traits identified in the IPIP: extraversion and openness.[191] Individuals scoring high on extraversion tend to be "energetic, active, talkative, sociable, outgoing, and enthusiastic."[192] Individuals scoring low on extraversion tend to be "shy, reserved, quiet, or withdrawn."[193] Similarly, individuals scoring high on openness tend to be "intellectually curious, sensitive to beauty, individualistic, imaginative, and

182. *Id.*

183. *See supra Subsection* II.D.1.a.

184. Shaun B. Spencer, *Privacy and Predictive Analytics in E-Commerce*, 49 NEW ENG. L. REV. 629, 633–38 (2015).

185. *See supra* Sections II.A–B.

186. S. C. Matz et al., *Psychological Targeting as an Effective Approach to Digital Mass Persuasion*, 114 PROC. NAT'L ACAD. SCI. U.S. 12714, 12715 (2017), https://www.pnas.org/content/pnas/114/48/12714.full.pdf.

187. *Id.* at 12714.

188. *Id.*

189. *Id.* at 12715.

190. *Id.* The myPersonality.org website indicates that it is no longer sharing data with researchers. *See MyPersonality Project*, MYPERSONALITY.ORG (May 2018), http://www.mypersonality.org.

191. Matz et al., *supra* note 186, at 12715.

192. *Id.*

193. *Id.*

unconventional," whereas individuals scoring low on openness tend to be "traditional and conservative and are likely to prefer the familiar over the unusual."[194]

Matz et al. then created advertisements designed to test each of the traits on two different products.[195] First, they created high-extraversion and low-extraversion ads for a cosmetics product.[196] The high-extraversion ad showed the protagonist at a party and the tagline, "Dance like no one's watching (but they totally are)."[197] The low-extraversion ad showed the protagonist applying the product while looking at herself in her mirror at home and the tagline, "Beauty doesn't have to shout."[198] They then placed these ads into the users' Facebook feeds while they browsed.[199] The results showed a statistically significant correlation between the users' extraversion and the nature of the message.[200] Users seeing the ad tailored to their high or low extraversion were 1.54 times more likely to purchase from the online store than users seeing the ad tailored toward the opposite preference.[201]

The researchers repeated the experiment with advertisements for a crossword puzzle app.[202] They created high-openness and low-openness ads and randomly placed them in the Facebook feeds of users with like patterns associated with either high or low openness.[203] The high-openness ad used a visual showing a dizzying mix of jumbled letter tiles in the shape of a cresting wave, and the following text: "Aristoteles?[204] The Seychelles?[205] Unleash your creativity and challenge your imagination with an unlimited number of crossword puzzles."[206] The low-openness ad used a visual showing two empty crossword puzzle boards, one on paper and one on a smart phone, with the text "Settle in with an all-time favorite! The crossword puzzle that has challenged players for generations."[207] As in the prior experiment, the results showed a statistically significant correlation between the users' openness and the nature of the message. Users seeing the ad tailored to their high or low openness were 1.38 times more likely to purchase

194. *Id.*
195. *Id.*
196. *Id.*
197. *Id.*
198. *Id.*
199. *Id.*
200. *Id.*
201. *Id.*
202. *Id.*
203. *Id.*
204. Aristoteles is a crater on the moon named using the classic form of Greek philosopher Aristotle's name. *See Aristoteles (Lunar Crater)*, SMITHSONIAN NAT'L AIR & SPACE MUSEUM, https://airandspace.si.edu/multimedia-gallery/web11614-2010640jpg (last visited Mar. 31, 2020).
205. The Seychelles are islands in the Indian Ocean that form the Republic of Seychelles. *See All About Seychelles*, AFRICA.COM, https://africa.com/heres-what-you-need-to-know-about-seychelles/ (last visited Mar. 31, 2020).
206. Matz et al., *supra* note 186, at 12715.
207. *Id.*

from the online store than users seeing the ad tailored toward the opposite preference.[208] The difference was far more pronounced for the low-openness ad than it was for the high-openness ad.[209]

In their final study, the researchers advertised a "bubble shooter" game to an audience of Facebook users who were already connected with a list of similar games.[210] They determined the users' psychological profile by mapping their Facebook Likes onto the likes in the myPersonality.com database and determined that the audience was highly introverted.[211] They then randomly assigned audience members to see either the company's standard ad or a low-extraversion ad.[212] The standard ad read, "Ready? FIRE! Grab the latest puzzle shooter now! Intense action and brain-bending puzzles!"[213] The low-extraversion ad read, "Phew! Hard day? How about a puzzle to wind down with?"[214] The results again showed that the tailored ad was more effective.[215] Users seeing the low-extraversion ad had a 1.3 times higher click-through rate and a 1.2 times higher conversion rate than users seeing the standard message.[216]

Although Matz et al.'s study exploited just a pair of personality traits, there is no reason why marketers could not apply a similar methodology to other types of biases and vulnerabilities. As described above, marketers can already use real-time analytics to identify whether subjects are particularly vulnerable to specific biases or psychological pressures.[217] Once the vulnerability is identified, the task of adapting marketing messages to exploit those biases and vulnerabilities differs little from the marketing practices currently fueled by online behavioral advertising. For example, Uber recently found that a low mobile device battery was among the strongest predictors of whether Uber users would pay higher surge prices, presumably because they fear being stranded with a dead battery.[218] Uber stated that it did not and does not use device battery life to set surge prices,[219] but any ride sharing service with real-time access to battery life data could easily exploit consumer anxiety about a dying battery to extract higher prices.

208. *Id.* at 12716.
209. *Id.*
210. *Id.* at 12716–17.
211. *Id.* at 12717.
212. *Id.*
213. *Id.*
214. *Id.*
215. *Id.*
216. *Id.*
217. *See supra* text accompanying notes 183–85.
218. *See* Shankar Vedantam & Maggie Penman, *This Is Your Brain on Uber*, HIDDEN BRAIN: NPR (May 17, 2016, 12:01 AM), https://www.npr.org/2016/05/17/478266839/this-is-your-brain-on-uber.
219. *Id.*

### *2. Creating and Then Exploiting Individual Vulnerabilities*

Marketers could go further still. Rather than discovering existing vulnerabilities, marketers could exacerbate or even create vulnerabilities in individual subjects and then exploit those vulnerabilities. For example, marketers could exploit the phenomenon of ego depletion to make subjects likely to make more purchases or more expensive purchases. Behavioral research into "ego depletion" has shown that self-control can be depleted by making a series of difficult choices or undertaking demanding cognitive tasks.[220] People are more likely to give into temptation and become more vulnerable to marketing messages while in a depleted state.[221] Baumeister et al. have shown that ego depletion can increase both impulse spending and the amount that consumers are willing to pay for goods.[222] In addition, subjects in a depleted state are more likely to rely on default options to guide their behavior.[223] Relying on this principle, online platforms and apps could make their privacy settings difficult to find and change, thus putting consumers who do attempt to change their settings into an ego-depleted state in which they may be more likely to accept low-privacy defaults or be persuaded by explanations of why sharing may benefit them.

Calo suggests that marketers could exploit ego depletion by counting how many decisions consumers made during the day and sending a consumer a text from the nearest donut shop at exactly the moment when the consumer was "least likely to resist."[224] Expanding on this approach, marketers or apps with frequent consumer contact could structure the user experience to deplete the consumer and then target the depleted consumer with offers and messages when the consumer is most vulnerable.

A Facebook experiment several years ago suggested one way that marketers could create biases or vulnerabilities in their subjects. Prior research had established that emotional states could be transferred to others by "emotional contagion."[225] Kramer et al. wanted to test whether emotional contagion could take place online without any direct user interaction.[226]

The researchers manipulated the amount of emotional expressions that subjects saw in their Facebook News Feeds.[227] They then tested whether "exposure to emotions led people to change their own posting behaviors, in particular whether exposure to emotional content led people to post content that was consistent with the exposure."[228] In one experiment, the researchers reduced people's exposure to positive emotional content from friends in their News Feed; in

220. KAHNEMAN, *supra* note 11, at 41–42.

221. *Id.* at 41, 81.

222. Roy F. Baumeister et al., *Free Will in Consumer Behavior: Self-control, Ego Depletion, and Choice*, 18 J. CONSUMER PSYCHOL. 4, 9 (2008).

223. *Id.*

224. Calo, *supra* note 7, at 996.

225. Adam D. I. Kramer et al., *Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks*, 111 PROC. NAT'L ACAD. SCI. U.S. 8788, 8788 (2014).

226. *Id.*

227. *Id.*

228. *Id.*

the other, the researchers reduced people's exposure to negative emotional content from friends in their News Feed.[229] The researchers then measured the positive and negative content of the subjects' own Facebook status updates.[230]

The researchers' findings were striking: "We show, via a massive (N = 689,003) experiment on Facebook, that emotional states can be transferred to others via emotional contagion, leading people to experience the same emotions without their awareness."[231] As the researchers recognized, although they analyzed only the subjects' Facebook posts, the subjects presumably experienced increased positive or negative emotions in other aspects of their lives: "Online messages influence our experience of emotions, which may affect a variety of offline behaviors."[232] Building on this methodology, online platforms could trigger or exacerbate various emotional states in their users and then allow marketers to exploit those emotional states with well-timed and tailored marketing offers.

## III. DEFINING MANIPULATION

Before assessing how to regulate manipulation, we must first define (1) what manipulation is, and (2) what kinds of manipulation are sufficiently harmful to merit potential regulation. Part III takes on the first task, while Part IV takes on the second.

This Part first surveys various definitions of manipulation proposed by other scholars. Next, this Part identifies conflicts and commonalities in those definitions. Finally, this Part offers my proposed definition of manipulation. As we shall see below, defining manipulation is challenging for several reasons. First, the line between traditionally acceptable "influence" techniques and unacceptably manipulative techniques is not obvious. Second, deciding whether a particular influence technique is "manipulative" may depend on some combination of the nature of the message itself, the influencer's knowledge about the subject's susceptibility to the message, the subject's lack of awareness of the mechanism of influence, and the subject's actual preferences or beliefs, most of which are may be unknowable in any given situation. Those challenges will inform Part V's description of the difficulties of regulating manipulation directly.

### *A. Prior Definitions of Manipulation*

Before considering the various proposed definitions, this Section begins with a discussion of the valuable way in which Susser, Roessler, and Nissenbaum framed their forthcoming study of manipulation.[233] They begin their definitional task by locating manipulation along a spectrum of influence techniques. On their

229. *Id.*
230. *Id.* at 8789.
231. *Id.* at 8788.
232. *Id.* at 8790.
233. Susser et al., *supra* note 5.

spectrum, the least troubling type of influence is persuasion, followed by manipulation, then deception and coercion.[234] They craft their definition of manipulation in part by distinguishing it from these other, perhaps more familiar, forms of influence.[235]

Distinguishing manipulation from coercion is straightforward. Susser et al. define coercion as "the restriction of acceptable options from which another person might choose."[236] Unlike coercion, which involves an explicit (albeit socially unacceptable) appeal to the subject's "capacity for conscious decision-making, manipulation attempts to subvert that capacity."[237] As they explain, coercion is overt, while manipulation is covert.[238]

Distinguishing manipulation from deception is a bit more difficult. Susser et al. define deception as causing someone to hold false beliefs.[239] Although deception may sometimes be a means of manipulation,[240] Susser et al. argue that deception is not the only means.[241] As they explain, one may influence a subject's choice without influencing the subject's beliefs by instead exploiting the subject's biases and vulnerabilities.[242]

The most challenging distinction, however, is between manipulation and persuasion. Susser et al. define persuasion as an appeal to the subject's conscious decision-making process.[243] Manipulation, by contrast, bypasses the subject's decision-making power.[244] Thus, they distinguish manipulation from persuasion because persuasion leaves the choice up to the subject, while manipulation subverts the subject's decision-making power.[245]

The fuzzy line between manipulation and persuasion will pose the most significant challenge to any attempt to regulate manipulation. Part II above detailed many techniques that marketers use or could use to exploit consumer biases and vulnerabilities. Any definition of manipulation must plausibly explain which techniques constitute mere persuasion and which constitute manipulation. With that backdrop in mind, let us turn to the definitions proposed to date.

Susser et al. define manipulation as an intentional[246] attempt to influence the subject that (1) is hidden from the subject, (2) attempts to exploit a subject's

234. *Id.* (manuscript at 10); a*ccord* Zarsky, *Privacy and Manipulation*, *supra* note 7, at 159 (identifying the need to distinguish manipulation from "fraud, misrepresentation, or simple coercion").

235. *See* Susser et al., *supra* note 5 (manuscript at 10); Zarsky, *Privacy and Manipulation*, *supra* note 7, at 159.

236. Susser et al., *supra* note 5 (manuscript at 2).

237. *Id.* (manuscript at 14).

238. *Id*.

239. *Id.* (manuscript at 17).

240. *Id.* (manuscript at 2, 17). Unlike Susser et al., I contend that any attempt to influence a subject by instilling a false belief should be considered deception but not manipulation.

241. *Id.* (manuscript at 18).

242. *Id.*

243. *Id.* (manuscript at 11).

244. *Id.* (manuscript at 13–14).

245. *Id.* (manuscript at 13–14, 22).

246. *Id.* (manuscript at 22).

"cognitive, emotional, or other decision-making vulnerabilities," and (3) is "targeted" at those vulnerabilities.[247] Susser et al. also observe, however, that the targeting and exploiting elements may be unnecessary to the definition, and that manipulation could simply be defined as any hidden influence.[248] They reason that targeting and exploiting the subject's vulnerabilities are simply the means by which the manipulator exerts the hidden influence.[249] They assert, however, that targeting exacerbates the manipulation and therefore creates more concern about the manipulative practice.[250]

Sunstein argues that "[a] statement or action can be counted [as] manipulative to the extent that it does not sufficiently engage or appeal to people's capacity for reflective and deliberative choice."[251] Sufficiency refers to the degree of reflection and deliberation involved, not to the justification for the manipulation.[252] "Thus defined, manipulation is a pervasive feature of human life. It is for this reason that while the legal system is generally able to handle lies and deception, it has a much harder time in targeting manipulation."[253] Sunstein acknowledges that the term "sufficiently" leaves much ambiguity.[254] Such ambiguity is intentional, he points out, because one cannot determine whether an attempted influence constitutes manipulation "without asking about the sufficiency of people's capacity to deliberate on the question at hand."[255] Sunstein also notes that there are degrees of manipulation depending on the extent to which the manipulator impairs deliberation—subliminal advertising bypasses it altogether, whereas other forms may simply influence deliberation by "triggering certain forms of automatic processing (for example, through framing a problem so as to provoke the desired response)."[256] Finally, Sunstein notes that the manipulation must be intentional.[257]

247. *Id.* (manuscript at 23). Ido Kilovaty adopts Susser et al.'s definition in his exploration of how data breach law could address manipulation in the political context. Kilovaty, *supra* note 8, at 471 (adopting Susser et al.'s definition of manipulation as "imposing a hidden influence on someone by targeting and exploiting their weaknesses or vulnerabilities").

248. Susser et al., *supra* note 5 (manuscript at 23). I suggest that defining manipulation as merely a hidden influence would not completely distinguish manipulation from deception. Although deception through a false or misleading statement would not be hidden from the subject, deception by omission would. *Cf.* RESTATEMENT (SECOND) OF TORTS § 551(1) (AM. LAW INST. 1977) ("One who fails to disclose to another a fact that he knows may justifiably induce the other to act or refrain from acting in a business transaction is subject to the same liability to the other as though he had represented the nonexistence of the matter that he has failed to disclose, if, but only if, he is under a duty to the other to exercise reasonable care to disclose the matter in question."). Hiddenness does, however, distinguish manipulation from persuasion and coercion, because both presume that the subject is aware of the influence. Susser et al., *supra* note 5 (manuscript at 13) (stating that "persuasion and coercion have in common that they attempt to influence us without undermining our decision-making powers").

249. Susser et al., *supra* note 5 (manuscript at 23).

250. *Id.*

251. Sunstein, *supra* note 5, at 239.

252. *Id.* at 217 n.3.

253. *Id.* at 239.

254. *Id.* at 216.

255. *Id.*

256. *Id.* at 217.

257. *Id.* at 218 & n.4.

Tal Zarsky's recent treatment of manipulation adopts Sunstein's definition of manipulative actions as "intentional measures that do not sufficiently engage or appeal to the individual's capacity for reflection and deliberation."[258] Zarsky notes that Sunstein drew on similar definitions of manipulation as an attempt to "bypass rational capacities and subvert decision-making."[259] As we shall see below, Zarsky also identifies several particularly troublesome features of manipulation in the Digital Age,[260] but those features do not change the broad definition of manipulation.

Zarsky also addressed the definition of manipulation in an earlier work.[261] Zarsky identified two potentially harmful forms of online influence. The first is false or deceptive advertising, which has drawn most of the regulatory attention.[262] The second, which Zarsky argued had yet to be seriously regulated, was advertising that is "manipulative and impede[s] the relevant consumer's autonomy."[263] Zarsky describes the potential harm from manipulative advertising as follows: "[W]hen consumers are bombarded with specially tailored marketing pitches and advertisements that will capitalize on their vulnerabilities and take advantage of their weaknesses, their subsequent actions might not be those that they would have chosen, should they have had the opportunity to reflect on these matters in solitude."[264] Thus, the tailoring in Zarsky's version of manipulation parallels the targeting in Susser et al.'s definition.[265] Similarly, the capitalization on consumers' vulnerabilities parallels the exploitation of vulnerabilities in Susser et al.'s definition.[266] In addition, the circumvention of the choice the consumer would have made upon undisturbed reflection parallels Sunstein's requirement that the influence insufficiently engage or appeal to people's capacity for reflection and deliberation.[267]

Ryan Calo's thorough examination of what he calls "digital market manipulation" does not propose a formal definition of manipulation.[268] Yet his description of Hanson and Kysar's work on market manipulation dovetails with Susser et al.'s definition.[269] Calo explains that, according to Hanson and Kysar, firms will use what they know about people's tendencies to act irrationally and will exploit those tendencies for their own gain.[270] Thus, Calo's model of manipula-

258. Zarsky, *Privacy and Manipulation*, *supra* note 7, at 160 (footnote omitted) (citing Sunstein, *supra* note 5, at 216).

259. *Id.*

260. *Id.* at 169.

261. Tal Z. Zarsky, *Online Privacy, Tailoring, and Persuasion*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION 209 (Katherine J. Strandburg & Daniela Stan Raicu eds., 2006) [hereinafter Zarsky, *Online Privacy*].

262. *Id.* at 216–19.

263. *Id.* at 219.

264. *Id.* at 220.

265. *Compare id.*, *with* Susser et al., *supra* note 5 (manuscript at 2).

266. *Id.*

267. Sunstein, *supra* note 5, at 216.

268. Calo, *supra* note 7.

269. *See id.* at 1001–03; Susser et al., *supra* note 5, at 22.

270. Calo, *supra* note 7, at 1001.

tion involves attempts to influence subjects by (1) targeting the subjects' tendencies to act irrationally and (2) exploiting those tendencies for the manipulators' own gain.[271] Those two features neatly track the targeting and exploiting components of Susser et al.'s definition.[272]

Eric Posner offered yet another definition of manipulation in his response to the Sunstein article discussed above.[273] He began with a dictionary definition: "to control or play upon by artful, unfair, or insidious means especially to one's own advantage."[274] In Posner's view, the manipulator knows that the subject brings "incorrect assumptions to a transaction and does not correct them, or else anticipates and takes advantage of people's propensity to make incorrect inferences."[275] Again, Posner's definition shares much in common with the targeting and exploiting vulnerabilities elements of Susser et al.'s definition.[276]

Becker & Feldman propose seven elements that must be present for a practice to constitute manipulation.[277] Four relate to the seller's knowledge and motivation; the seller must be aware of the vulnerability, be able to exploit the vulnerability, have a profit motive, and be prepared to ignore the consumer's self-interest if necessary.[278] Two relate to the exploitative tactic, which must be unrelated to the product or its features and must not be a "natural byproduct" of the market activity.[279] The last relates to the consumer, who must be unaware of the tactic or at least be unaware of how it affects her behavior.[280]

Finally, Harris and Albin offered a definition of manipulation, though they limited it to the context of consumer lending. They defined manipulation as a lender's attempt to lead a "consumer to borrow . . . through exploitation of . . . [the consumer's] biases and illusions, heuristics, inability to perform complex calculations, lack of relevant information, or a state of mind in which not enough cognitive resources are allocated to the decision."[281] Unlike the other definitions, Harris and Albin's does not require that the lender intend to manipulate or be "aware of the cognitive processes that allow manipulation."[282]

271. *See id.*
272. Susser et al., *supra* note 5, at 22–23.
273. Eric A. Posner, *The Law, Economics, and Psychology of Manipulation* (Coase-Sandor Inst. for Law & Econ., Working Paper No. 726, 2015), http://ssrn.com/abstract=2617481.
274. *Id.* at 1.
275. *Id.*
276. *See id.*; Susser et al., *supra* note 5, at 22–23.
277. Becher & Feldman, *supra* note 19, at 475.
278. *Id.*
279. *Id.*
280. *Id. at* 476.
281. Harris & Albin, *supra* note 17, at 443.
282. *Id.*

### *B. A Proposed Definition of Manipulation*

The definitions above may not be identical, but they share several features.[283] First, they all contain the notion of circumventing the subject's rational decision-making process. Sunstein and Zarsky refer to this as "insufficient" engagement of the subject's capacity for deliberative choice.[284] Susser et al., Calo, Posner, and Harris & Albin describe this element more narrowly as exploiting the subject's weaknesses or vulnerabilities.[285] As Susser et al. explain, Sunstein's "insufficiency" element injects a normative judgment of the influence technique that undermines Sunstein's definition.[286] In contrast, Susser et al.'s requirement that the manipulator exploit the subject's vulnerability can be understood as a signal that the subject's capacity for rational choice has was not "sufficiently" engaged.[287]

Second, all but one of these definitions require intent by the alleged manipulator. Susser et al., Sunstein, Zarsky, and Becher & Feldman explicitly require intent to manipulate the subject.[288] In addition, both Calo's and Posner's treatment of manipulation involve an element of intentionality.[289] Calo's understanding presumes that the manipulator targets and exploits the subject's tendency to act irrationally,[290] which suggests that the manipulator does so intentionally. And Posner's understanding assumes that the manipulator takes advantage of the subject's incorrect assumptions or the subject's propensity to make incorrect inferences,[291] which again suggests that the manipulator does so intentionally. Only Harris & Albin's definition allows for manipulation without intent.[292]

Susser et al. include one requirement that does not appear in the other definitions. They require that the influence be "hidden."[293] They recognize that Sunstein disagrees with them on this point,[294] and on this score Sunstein appears to have the better of the argument. Sunstein argues that "[s]ome acts can be both

283. Two elements appear only in Becher and Feldman's formulation: the requirement that the manipulator have a profit motive and the requirement that the manipulator be willing to ignore the consumer's self-interest. Becher & Feldman, *supra* note 19, at 475. This Article does not treat those features as a necessary element of manipulation, though they may be relevant to determining what types of manipulation merit a regulatory response. *See infra* Part IV.

284. Sunstein, *supra* note 5, at 220; Zarsky, *Privacy and Manipulation*, *supra* note 7, at 160.

285. Calo, *supra* note 7, at 1034; Harris & Albin, *supra* note 17, at 443; Posner, *supra* note 6, at 1; Susser et al., *supra* note 5, at 2.

286. Susser et al., *supra* note 5, at 20.

287. *Id.* at 2.

288. Becher & Feldman, *supra* note 19, at 475; Sunstein, *supra* note 5, at 216, 218 n.4; Susser et al., *supra* note 5, at 22; Zarsky, *Privacy and Manipulation*, *supra* note 7, at 160; *accord* Sunstein, *supra* note 5, at 220 (describing philosophical accounts of manipulation that require intent).

289. *See* Calo, *supra* note 7, at 1001; Posner, *supra* note 6, at 1.

290. *See* Calo, *supra* note 7, at 1001.

291. Posner, *supra* note 6, at 1.

292. Harris & Albin, *supra* note 17, at 443 (stating that the manipulator need not intend to manipulate or know of the cognitive vulnerability).

293. Susser et al., *supra* note 5, at 2, 16, 20.

294. *Id.* at 20; *see also* Sunstein, *supra* note 5, at 231.

manipulative and fully revealed to those who are being manipulated."[295] For example, a graphic health warning that plays on consumer biases would still be perfectly visible to consumers.[296]

I contend that one can best rationalize Susser et al. and Sunstein's approaches to "hiddenness" by clarifying what must be hidden—the manipulative stimulus or the manipulative mechanism. For example, an actor trying to exploit the anchoring bias must make the anchor visible to the subject.[297] This anchor is the stimulus, and it cannot be hidden. What is hidden from the subject, however, is the manipulative mechanism—the cognitive process that drives her estimate toward the anchor.[298] Indeed, the subconscious nature of manipulation is one reason why manipulation is so powerful.[299] This interpretation preserves the core of what Susser et al. understand to be the distinction between persuasion and manipulation. Persuasion is a "forthright appeal" to the subject's decision-making power, while manipulation circumvents that power.[300] Regardless of whether the manipulative stimulus is visible or hidden, if the subject does not know how or why the stimulus affects her decision making, then her decision-making power remains subverted.

In light of the foregoing discussion, I propose the following definition: manipulation is an intentional attempt to influence a subject's behavior by exploiting a bias or vulnerability.[301] This definition of manipulation incorporates the shared features of prior scholars' definitions. It requires intent to influence the subject, which appears in all but one of the prior definitions. And it requires a subversion of the decision-making process, which is shared in various forms by all of the definitions. Sunstein framed this requirement quite broadly as insufficiently engaging the subject's capacity for rational choice, whereas Susser et al. framed the requirement more narrowly as exploiting the subject's decision-making vulnerabilities.[302] My proposed reference to "biases and vulnerabilities" hews closer to Susser et al.'s narrower formulation.[303] Finally, my earlier rationalization of the Susser et al./Sunstein debate over the hiddenness of the manipulation is embedded in my requirement that there be a bias or vulnerability.[304] The presence of the bias or vulnerability means that the mechanism of influence will be hidden from the subject, even if the stimulus is visible.

The mere fact that an act is manipulative, however, does not mean that the law should prohibit it. Indeed, manipulation has been commonplace in many

295. Sunstein, *supra* note 5, at 231.

296. *Id.*; Susser et al., *supra* note 5, at 20.

297. *See supra* text accompanying note 35.

298. *Id.*

299. *See* CIALDINI, INFLUENCE, *supra* note 14, at 11.

300. Susser et al., *supra* note 5, at 2, 13.

301. Obviously such a definition is not limited to the commercial context. Although this Article focuses on the practice and potential regulation of consumer manipulation, manipulation can occur in many contexts. *E.g.* THALER & SUNSTEIN, *supra* note 15, at 6 (discussing manipulation by government as well as private institutions); Susser et. al, *supra* note 5, at 5–7 (describing manipulation of employees and voters).

302. Sunstein, *supra* note 5, at 216; Susser et al., *supra* note 5, at 2.

303. *See* Susser et al., *supra* note 5, at 2.

304. *See id.* at 20; Sunstein, *supra* note 5, at 231.

contexts for decades without any regulation.[305] The next Part, therefore, considers when we should consider regulating online manipulation of consumers.

## IV. THE CASE FOR REGULATING ONLINE MANIPULATION

This Part considers why online manipulation justifies exploring some form of regulatory response. Before considering the threat posed by online manipulation, we should review the reasons why manipulation is harmful, whether online or offline. First, manipulation harms autonomy because it undermines people's decision-making agency.[306] Second, manipulation leads to inefficient outcomes by leading people to make choices inconsistent with their actual preferences.[307] Third, when it enters the political arena, manipulation undermines democratic deliberation.[308] Finally, manipulation harms people's dignity by treating people as experimental subjects and mere means to an end.[309] Online manipulation poses all of these harms, of course, but scholars have articulated persuasive reasons why online manipulation is particularly harmful.

Calo offers the most thorough account of the harm from online manipulation.[310] He explains why the "digitization of commerce dramatically alters the capacity of firms to influence consumers at a personal level."[311] Digital consumers are technologically "mediated" consumers, in the sense that they approach the marketplace through technology designed by someone else.[312] This mediation, Calo argues, has three important consequences that facilitate digital market manipulation. First, "technology captures and retains intelligence on the consumer's interaction with a given firm."[313] Second, "firms can and do design every aspect of the interaction with the consumer."[314] Finally, "firms can in-

305. *See* VANCE PACKARD, THE HIDDEN PERSUADERS (1957) (describing advertising research as far back as the 1940s concerning "techniques designed to reach the unconscious or subconscious mind because preferences generally are determined by factors of which the individual is not conscious"); Sunstein, *supra* note 5, at 219 ("Because of the pervasiveness of manipulation, and because it often does little or no harm, the legal system usually does not attempt to prevent it. At least in general, the costs of regulating manipulation would far exceed the benefits."); Zarsky, *Privacy and Manipulation*, *supra* note 7, at 171 ("advertising has always relied on various forms of manipulation").

306. Kilovaty, *supra* note 8, at 477; Sunstein, *supra* note 5, at 217; Zarsky, *Privacy and Manipulation*, *supra* note 7, at 174 (defining autonomy as "the ability to make informed decisions regarding one's life, while choosing between several reasonable options") (citing GERALD DWORKIN, THE THEORY AND PRACTICE OF AUTONOMY (1988)).

307. Zarsky, *Privacy and Manipulation*, *supra* note 7, at 172–73; *cf.* Sunstein, *supra* note 5, at 218 (noting that the welfarist objection to manipulation is uncertain because some manipulations can be beneficial).

308. Kilovaty, *supra* note 8, at 479–80.

309. Kilovaty, *supra* note 8, at 483–84; Sunstein, *supra* note 5, at 217; Zarsky, *Privacy and Manipulation*, *supra* note 7, at 175.

310. Calo, *supra* note 7, at 999–1004.

311. *Id.* at 999.

312. *Id.* at 1003.

313. *Id.*; *accord* Susser et al., *supra* note 5, at 2 ("First, widespread digital surveillance makes it easy for data collectors and aggregators to identify our weaknesses.").

314. Calo, *supra* note 7, at 1004; *accord* Susser et al., *supra* note 5, at 2 ("Second, digital platforms offer a perfect medium through which to leverage those insights.").

creasingly choose when to approach consumers, rather than wait until the consumer has decided to enter a market context."[315] Calo also argues that the vast data collection, sophisticated analytics, and hyper-personalization possible in the digital marketplace dramatically expand the potential for manipulation online.[316]

Similarly, Zarsky identifies four troubling features of Digital Age manipulation. First, Digital Age manipulation can be individually tailored to each subject based on pervasive data collection.[317] Second, Digital Age manipulation can adapt to the subject's responses to the manipulation, "thus rendering manipulation an ongoing process."[318] Third, Digital Age manipulation is not transparent to the subject.[319] Finally, Digital Age manipulation will continually improve as advanced data analytics show what interventions are effective over time.[320]

Calo also anticipates the argument that digital market manipulation does not cause any actual consumer harm. He notes that digital market manipulation "generates externalities and decreases overall market efficiency,"[321] as well as subjective and objective privacy harm.[322] Subjective privacy harm arises from consumers' vague sense that information is being collected against them and used to their disadvantage.[323] Objective privacy harm arises when firms manipulate consumers to extract benefits they might not otherwise provide.[324]

Marketers may note, correctly, that they have engaged in manipulative techniques for decades, relying on cognitive biases and psychological influences that are present in some subset of the population.[325] In the case of such "scattershot" manipulation, some consumers will be susceptible to the bias or vulnerability at issue, but many others will not.[326] In contrast, personalized online manipulation will target the consumers most susceptible to manipulation. Marketers may suggest that, if it was permissible to market to a broad range of consumers, only some of whom would be susceptible to a particular cognitive bias, it should also be permissible to market only to the subset of consumers who actually are susceptible. Put differently, marketers may suggest that regulating personalized digital manipulation amounts to punishing marketers for tailoring their messages too well.

Such arguments, however, ignore the fact that the core justification for regulating online manipulation rests in the personalization that the Digital Age makes possible. Online manipulation uses the consumer's own behavioral data against her to circumvent her rational decision-making process. In this way,

315. Calo, *supra* note 7, at 1004.
316. *Id.* at 1006–08.
317. Zarsky, *Privacy and Manipulation*, *supra* note 7, at 169; *accord* Susser et al., *supra* note 5, at 2.
318. Zarsky, *Privacy and Manipulation*, *supra* note 7, at 169.
319. *Id.* Non-transparency, however, is not unique to Digital Age manipulation. *See supra* text accompanying notes 54–104.
320. Zarsky, *Privacy and Manipulation*, *supra* note 7, at 169.
321. Calo, *supra* note 7, at 1027.
322. *Id.* at 1029.
323. *Id.*
324. *Id.*
325. *See supra* Section II.B.
326. *See* Calo, *supra* note 7, at 1014.

online manipulation is more threatening to consumers than the existing online behavioral advertising, in which our behavioral data may be used to decide the types of ads we see or offers we receive, but does not undermine our ability to assess those ads and offers. That is the essential difference between scattershot manipulation and the type of personalized manipulation possible in the Digital Age.

Of course, regulating all online manipulation would be impractical from a political perspective and unnecessary from a consumer protection perspective. As we have already seen above, marketers have been attempting to use manipulative techniques for decades without regulation and without significant objections.[327] Instead, any attempt to regulate online manipulation should focus on the extreme personalization that makes online manipulation so troubling.

To accomplish this goal, any attempted regulation should focus on online manipulation with the following features. First, the attempted influence must be likely to exploit an individual consumer's biases or vulnerabilities. This requirement limits the regulation to practices aimed at individual consumers, rather than the scattershot manipulation that predates the Digital Age. Second, the influencer must act with intent to exploit the individual consumer's biases or vulnerabilities. This requirement preserves the intent element from proposed definition of manipulation. Finally, the attempted influence must be undertaken for the marketer's advantage. This requirement limits the regulation to situations likely to distort the market and facilitate rent seeking.[328] As we shall see in Part V, however, a number of definitional challenges make direct regulation of online manipulation impractical, if not impossible.

## V. CHALLENGES INHERENT IN DIRECT REGULATION OF ONLINE MANIPULATION

This Part identifies the challenges involved in drafting direct regulation of online manipulation. Direct regulation could take many different forms. At the most extreme, it could prohibit all online manipulation.[329] Alternatively, it could involve consent or disclosure requirements.[330] Such prohibitions or requirements could be enforceable by administrative agencies[331] or through private rights of

327. *Id.* at 1024.

328. *Id.* at 1022–23 (suggesting that we should only regulate online manipulation when "the incentives of firms and consumers are not aligned" because manipulation in this condition of misalignment leads to the extraction of "social surplus"); *see also* Zarsky, *Privacy and Manipulation*, *supra* note 7, at 172 (noting the welfarist argument that manipulation creates inefficient outcomes).

329. *Cf.* Calo, *supra* note 7, at 1041–42 (noting the possibility of "command and control" regulation of online manipulation, but also noting the risk of unintended consequences and First Amendment problems).

330. *Id.* at 1044 (noting that mandatory disclosure is possible but could be ineffective, in part because marketers would likely figure out how to draft compliant yet minimally effective disclosures, and in part because some studies suggest that telling subjects about the manipulation may not reduce its impact); *see also id.* at 1045–46 (suggesting that private companies conducting consumer research at scale be required to form internal committees to review research practices).

331. *Cf.* Calo, *supra* note 7, at 1043 (noting that FTC unfairness jurisdiction is not well suited to addressing the digital market manipulation problem because consumers might avoid the harm with effort, and because the harm is "not of the variety usually countenanced by agencies or courts"); *cf.* Eliza Mik, *The Erosion of Autonomy*

action. But none of these forms of direct regulation are possible without codifying a definition of the online manipulation to be regulated. That definitional exercise presents significant drafting challenges.

### *A. Defining Bias or Vulnerability*

Direct regulation of online manipulation may be impossible without first defining what constitutes a bias or vulnerability. That task, however, may prove to be the most difficult part of codifying manipulation.[332] As shown above, there are many different biases and vulnerabilities that could foster manipulation.[333] Some relate to judgments about how we make estimates, assign values, and assess risks.[334] Others relate to the types of psychological pressures that lead us to make decisions[335] or the ways that personality preferences predispose us to particular influences.[336] Still others relate to how we are affected by the sounds, colors, and layout of our physical and digital environment.[337] Even within each of those disciplines, scholars do not agree on a single set of biases and vulnerabilities,[338] so crafting a legal definition that would capture them all would likely be impossible.

Accordingly, rather than defining the specific characteristics of manipulation, one might instead define it with reference to its effects. Such an approach might incorporate Sunstein's definition by characterizing manipulation as a practice that bypasses the subject's "capacity for reflection and deliberation."[339] But the universe of practices falling into that category seems almost limitless. Indeed, deception would fall within that category because the falsehood circumvents the subject's deliberative process. Additionally, the range of capacity for reflection and deliberation likely varies widely across consumers, so such a definition might mean that the same marketing message was manipulative as to one consumer but not manipulative as to another.

Yet another alternative might be to look to the marketer's own internal processes to find a proxy for manipulation. Under this approach, the statute would presume that a bias or vulnerability exists if the marketer performed research to

*in Online Consumer Transactions*, 8 L. INNOVATION & TECH. 1, 33 (2016) (describing the regulatory scheme under The European Union's Directive on Unfair Commercial Practices, Directive 2005/29/EC, wherein a "material distortion" does not require proof of actual distortion; instead, the practice need only be capable of having such an effect).

332. *See* Zarsky, *Privacy and Manipulation*, *supra* note 7, at 169 ("Suffice it to say that precisely drawing the boundaries of such unacceptable [manipulative] actions is a challenge and will be left for another time (and paper).").

333. *See supra* Section II.A.

334. *See, e.g.*, KAHNEMAN, *supra* note 11, at 13–14.

335. *See, e.g.*, CIALDINI, INFLUENCE, *supra* note 14, at xiii.

336. *See, e.g.*, Matz et al., *supra* note 186, at 12714.

337. Becher & Feldman, *supra* note 19, at 477–79; s*ee, e.g.*, Hanson & Kysar, *Some Evidence of Market Manipulation*, *supra* note 64, at 1445–49.

338. *See, e.g.*, Peter B.M. Vranas, *Gigerenzer's Normative Critique of Kahneman & Tversky*, 76 COGNITION 179, 179–80 (2000) (describing empirical, methodological, and normative critiques of aspects of Kahneman and Tversky's heuristics and biases).

339. Sunstein, *supra* note 5, at 216.

determine whether a particular stimulus was likely to affect the decision or judgment of subjects who share particular behaviors or characteristics. Such an approach would avoid the need to describe, whether in specific or general terms, the cognitive or psychological mechanisms through which biases or vulnerabilities work. But it would also sweep in influence techniques that we have never before felt the need to regulate. For example, a test showing that an ad is more successful when it includes a puppy seems unobjectionable. But the approach contemplated in this paragraph could classify such an ad as manipulative.

In short, the difficulty of defining the tools of manipulation may render direct regulation of online manipulation impossible.

### *B. Defining Intent to Exploit the Bias or Vulnerability*

Assuming that one could define a bias or vulnerability, the next challenge would be how to describe the merchant's intent to exploit the bias or vulnerability. This task would be less challenging than the previous one. The regulation could simply require that the merchant knew of a bias or vulnerability and used a stimulus that the merchant knew or should have known that was likely to influence the consumer. A marketer engaged in personalized online manipulation would surely be using online behavioral advertising to identify profiles and deciding what stimulus to provide by reference to research identifying biases or vulnerabilities more likely to affect consumers with those profiles.

A potential loophole, however, would exist in such a regulation. Several scholars have pointed out the possibility that marketers need not search for specific biases or vulnerabilities to exploit.[340] Instead, using A/B testing, marketers could experiment with multiple versions of an advertisement or interface to see which one prompts the best consumer response. In such a situation, marketers need not intend or even know of any bias or vulnerability, and may not know why one advertisement or interface is more successful than the other.[341]

I contend that, in such a situation involving A/B testing, allowing the marketer to escape the regulation is acceptable. If the marketer truly does not know that there is a bias or vulnerability at work, then regulating that conduct would not advance the purpose of prohibiting intentional exploitation. And, to the extent that a clever marketer could conceal intentional exploitation beneath the cloak of A/B testing and hide any evidence that it was targeting a specific bias or vulnerability, that would constitute an acceptable loss.

340. *See* Maurits Kaptein et al., *Personalizing Persuasive Technologies: Explicit and Implicit Personalization Using Persuasion Profiles*, 77 INT'L J. HUMAN-COMPUTER STUD. 38, 38 (2015).

341. *See* Calo, *supra* note 7, at 1015.

### *C. Defining the Specificity with Which the Influencer Must Target the Consumer's Vulnerability*

Yet another challenge will involve how specifically the influencer must target the consumer's bias or vulnerability. This targeting requirement can be implemented in several different ways. The narrowest formulation would be to regulate only if the influencer gathered behavioral information from the consumer demonstrating the consumer's responses to prior uses of particular biases or vulnerabilities. This would reach the emerging body of "persuasion profiling" research that Calo identifies.[342] Persuasion profiling allows marketers use a consumer's responses to various attempted influence methods and build a profile predicting which methods are likely to influence that consumer.[343] For example, a marketer could track how consumers respond to advertisements implementing different types of influence techniques and then use those responses to predict successful influence techniques for each consumer.[344]

There are, however, many potential approaches to manipulation that do not rely on consumers' responses to specific types of influence techniques. Instead, these broader approaches gather online behavioral data to build broad profiles revealing personality traits[345] or cognitive styles.[346] Marketers would then use those profiles to predict which biases or vulnerabilities they could best exploit with particular consumers.

To reach this type of manipulation would require broader regulation. A moderately broader approach would find sufficient targeting when the marketer has determined that (1) an identifiable group (*e.g.*, people who share a personality trait) is susceptible to a particular bias or vulnerability and (2) the consumer is a member of that group. This middle ground standard would reach manipulation in which marketers used consumers' behavioral data against them, but would exempt "scattershot manipulation" of the type that has been practiced for many decades, in which marketers rely on biases and vulnerabilities that are prevalent to varying degrees in the overall population. This standard, however, could raise difficult issues of proof concerning the degree to which a marketer knew that a particular group was susceptible to a particular bias or vulnerability.

To overcome that problem of proof, the regulation could reach even more broadly and find sufficient targeting whenever the marketer decided to deliver information to a consumer based on information about that consumer. This standard would effectively presume that, if the marketer tailored a message to the consumer, then the marketer did so because it believed the consumer would be susceptible to a bias or vulnerability. Given the nature of online behavioral advertising, that would be an easy requirement to meet, since such ads are served

342. *Id.* at 1017.

343. Kaptein et al., *supra* note 340, at 38.

344. *Id.* at 38, 41.

345. *E.g.*, Matz et al., *supra* note 186, at 12714.

346. *See* Calo, *supra* note 7, at 1017 (citing John R. Hauser et al., *Website Morphing*, 28 MARKETING SCI. 202, 202–06 (2009) (describing how to alter, or "morph," website layouts based on each consumer's cognitive style)).

to particular users after algorithmically assessing the users' profiles.[347] Such a requirement would apply to all types of online behavioral advertising, but because of the requirement above of a particular bias or vulnerability in the consumer, the regulation would reach only potentially manipulative practices. On the other hand, marketers would remain free to use the "scattershot manipulation" that has been in use for decades.[348]

### *D. Requiring Causation and Harm*

Any direct regulation of online manipulation would likely require proof that the manipulation caused harm.[349] For several reasons, however, it will be difficult, if not impossible, to establish that the allegedly manipulative stimulus caused the consumer harm. First, although everyone has cognitive biases, "not everyone has the *same* biases or experiences them to the same degree."[350] In addition, even a well-established cognitive bias does not affect every subject.[351] Instead, in any given test of these biases, many subjects remain unaffected by the bias.[352] If you imagine a marketing test establishing that exploiting a particular bias or vulnerability increased sales compared to a control group, there are surely many people in the treatment group who do not make a purchase. The biases and vulnerabilities are not magic wands. Thus, it is impossible to conclude that mere exposure to a stimulus targeting a specific bias or vulnerability automatically affects the subject's judgment.

Next, it may be impossible to know whether the consumer would have made the purchase even without being exposed to the stimulus. Again, if you imagine a marketing test establishing that exploiting a particular bias or vulnerability increased sales, there are surely subjects in the control group who make a purchase despite not being exposed to the manipulative stimulus. And there are surely subjects in the treatment group who would have made the purchase anyway, even if they had not been exposed to the stimulus. Individual consumers bring their own unique sets of preferences to each transaction, and regulators would be hard pressed to identify a consumer's preference in any given situation.

One way to deal with these causation and harm problems is to omit the requirements entirely. That would likely preclude regulation through a private

347. Dacia Green, *Big Brother Is Listening to You: Digital Eavesdropping in the Advertising Industry*, 16 DUKE L. & TECH. REV. 352, 364–67 (2017).

348. ROBERT MANDEL, STRATEGIC AMBIGUITY, DECEPTION, AND SURPRISE IN AN AGE OF INFORMATION OVERLOAD GLOBAL DATA SHOCK (Stanford Univ. Press) (2019).

349. *See, e.g.*, *FTC Policy Statement on Deception*, F.T.C. (Oct. 14, 1983), https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception (stating that an act or practice is deceptive if it is likely to mislead consumers acting reasonably under the circumstances and is material to consumers–that is, it would likely affect the consumer's conduct or decisions with regard to a product or service); *FTC Policy Statement on Unfairness*, F.T.C. (Dec. 17, 1980) https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness (stating that an act or practice is unfair when it causes or is likely to cause substantial injury to consumers, cannot be reasonably avoided by consumers, and is not outweighed by countervailing benefits to consumers or to competition).

350. Calo, *supra* note 7, at 1014.

351. *Id.*

352. *Id.*

right of action, because it is difficult to envision enforcement schemes where private actors can sue despite being unable to show any causal link between the allegedly wrongful conduct and any effect on their behavior. In addition, the lack of causal connection between the prohibited conduct and consumer harm would likely doom any private right of action in federal court due to lack of standing.[353] Moreover, even as to direct regulation without a private right of action, the lack of causation and harm requirements would drastically weaken the justification for administrative enforcement.

### *E. Overcoming Practical Enforcement Challenges*

As a practical matter, consumers will not notice these manipulations. By design, the manipulations should not be noticeable. Though consumers may see the stimulus, they will rarely understand the manipulative mechanisms at work. And each consumer will see only the version tailored to them, so consumers are not in a position to spot a manipulative pattern.

Nor will regulators or watchdogs be poised to spot manipulative patterns in online marketing, because each visitor to a website may be shown a different offer, advertisement, or version of the website. In addition, the advertisements being served and tailored for manipulative purposes may not even be served on a single website; instead, they may be distributed across many different sites through third-party advertising networks.[354] It is certainly possible for a motivated and well-resourced watchdog or regulator to manufacture teams of dummy profiles to test for suspected manipulation, but they cannot be expected to discover more than a small slice of the actual manipulation.

### *F. Anticipating First Amendment Challenges*

Direct regulation of online manipulation would surely trigger a First Amendment challenge. It may be tempting to limit the regulation to manipulation for marketing purposes so that the law will be subjected to the lower degree of scrutiny applied to commercial speech.[355] Targeting marketers, however, could actually increase the law's vulnerability to a First Amendment challenge. In *Sorrell v. IMS Health Inc.*, the Supreme Court upheld a First Amendment challenge

353. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) (noting that plaintiff "could not, for example, allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III"). For a discussion of various standing requirements in state courts, see Wyatt Sassman, *A Survey of Constitutional Standing in State Courts*, 8 KY. J. EQUINE, AGRIC., & NAT. RESOURCES L. 349, 351 (2015).

354. *See* Bennett, *supra* note 112, at 901.

355. There are, however, many scholars and judges advocating increased protection for commercial speech and even suggesting that commercial speech should receive the same measure of protection as non-commercial speech. *See, e.g.*, Micah L. Berman, *Manipulative Marketing and the First Amendment*, 103 GEO. L.J. 497, 509 (2015) ("The cases following *Central Hudson* have gradually moved in the direction of stricter and stricter review of limits on commercial speech . . . ."); Neil Gormley, *Greening the Law of Advertising: Prospects and Problems*, 42 TEX. ENVTL. L.J. 27, 46 (2011) ("[T]he doctrinal winds have been blowing in the opposite direction—towards greater protection of commercial speech, not less.").

to a Vermont law intended to limit the process, called "detailing," that drug manufacturing companies use to market their drugs directly to physicians.[356] Pharmacies receive "prescriber-identifying" information when they process prescriptions, and many pharmacies sell this information to data miners who in turn lease the information to pharmaceutical manufactures who use it to improve their detailing efforts.[357] The Vermont law prohibited pharmacies from selling prescriber-identifying information or permitting prescriber-identifying information to be used for marketing prescription drugs without the prescriber's consent.[358] The law also prohibited drug manufacturers from using prescriber-identifying information for marketing prescription drugs without the prescriber's consent.[359] The statute contained exceptions allowing disclosure or use of prescriber-identifying information without the prescriber's consent for purposes such as health care research, enforcing compliance with preferred drug lists, educational communications to patients about care management, law enforcement operations, and other purposes provided by law.[360] The Court reasoned that, by limiting marketing uses but allowing exceptions for many other uses, the statute was not sufficiently tailored to the asserted governmental interest in keeping prescriber-identifying information private.[361] In addition, the Court reasoned that prohibiting only marketing uses rendered the statute a content-based and speaker-based restriction, which would require First Amendment scrutiny even if the statute were not a regulation of protected speech.[362] Thus, focusing on manipulative marketing may end up hurting the law's chances of surviving a First Amendment challenge.

If the traditional *Central Hudson* test were to apply, the most effective defense of an anti-manipulation regulation would be to style manipulation as a form of misleading consumers.[363] Under the *Central Hudson* test, if the speech concerns lawful activity and is not misleading, then the government must show that the regulation is supported by a substantial governmental interest, "directly advances the governmental interest asserted," and "is not more extensive than necessary to serve that interest."[364]

Calo argues that manipulation should fall outside of the *Central Hudson* test's coverage because manipulation "does not just tend to mislead; misleading is the entire point."[365] Calo points out that the Supreme Court has declined to extend First Amendment protection to in-person solicitation by lawyers.[366] In

356. 564 U.S. 552, 557–58 (2011).
357. *Id.* at 558.
358. *Id.* at 558–59.
359. *Id.* at 559.
360. *Id.* at 559–60.
361. *Id.* at 572.
362. *Id.* at 570–71.
363. *See* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y, 447 U.S. 557, 597 (1980).
364. *Id.* at 566.
365. Calo, *supra* note 7, at 1038; *cf.* Zarsky, *supra* note 7, at 179 (noting and rejecting the argument that manipulative communications should not be considered speech because they do not attempt to communicate information).
366. Calo, *supra* note 7, at 1038–39.

*Ohralik v. Ohio State Bar Association*,[367] the Supreme Court upheld state bar limitations on in-person solicitation because the pressures of in-person solicitation could discourage potential clients from "a critical comparison of the 'availability, nature, and prices' of legal services," and thereby undermine "informed and reliable decisionmaking."[368] Calo suggests that online manipulation may be equally or more influential than in-person solicitation by lawyers or their agents, and therefore should be considered misleading for *Central Hudson* purposes.[369] In addition, Kilovaty notes that scholars are developing the argument that the First Amendment should not bar regulation of manipulative speech because influencing subjects through often unconscious mechanisms is different from using traditional speech to convince them.[370]

## VI. CONCLUSION

The significant definitional and practical challenges above offer some reasons why we might decide not to pursue direct regulation of online manipulation. There is, however, a more compelling reason: direct regulation would attack the wrong problem.

In light of the long history of marketing manipulation before the Digital Age, I contend that the core problem with online manipulation is not its manipulative nature. Before the rise of online behavioral advertising, we heard little outcry about manipulation.[371] Instead, what has driven the recent calls for regulation is the dramatic increase in manipulative potential in the Digital Age, which allows marketers to tailor manipulations to individual users, in real time, on a

367. 436 U.S. 447 (1978).

368. *Id.* at 457–58.

369. Calo, *supra* note 7, at 1039. For an expansive argument that regulation of "behaviorally manipulative advertisements" should not be subject to the *Central Hudson* test because it is misleading, see Gormley, *supra* note 355, at 50–57.

370. Kilovaty, *supra* note 8, at 508 (citing Micah Berman, *Manipulative Marketing and the First Amendment*, 103 GEO. L.J. 497, 546 (2015)). Part VI proposes indirect regulatory efforts that would limit the data flows that make manipulation possible. Some argue that such efforts should not trigger First Amendment scrutiny because they do not regulate speech. *See* Calo, *supra* note 7, at 1035 (noting that limiting the data collection upon which online manipulators rely would not violate the First Amendment). Others argue, however, that data transfers are speech. Calo, *supra* note 7, at 1036 (citing Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57 (2014)). It seems that the "data-is-speech" side of the argument has prevailed. In *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011), a six-justice majority of the Supreme Court rejected the argument that data transfers are not speech. Vermont argued that its law should not be subject to First Amendment scrutiny because the law merely regulated conduct—the sale, transfer, and use of information—rather than speech. *Id.* at 567. The Court noted that it did not need to decide whether data sharing was speech because Vermont's law ultimately imposed content-based and speaker-based burdens on protected expression—the pharmaceutical manufacturers' detailing efforts. *Id.* at 571. In dicta, however, the Court signaled that restrictions on data sharing would likely constitute speech entitled to First Amendment protection. *Id.* at 570 ("Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs. There is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes.").

371. The calls for advertising reform focused instead on deceptive advertising. TIM WU, THE ATTENTION MERCHANTS: THE EPIC SCRAMBLE TO GET INSIDE OUR HEADS 189–90, 209 (2016). One exception was Vance Packard's 1957 book, *The Hidden Persuaders*. PACKARD, *supra* note 305, at 6.

massive scale.[372] Recent objections to online manipulation cite the intense datafication, personalization, and real-time implementation made possible in the Digital Age.[373] For that reason, I contend that the real problem with online manipulation is its online implementation.

Online manipulation is just one of many potentially harmful uses of consumer data in the Digital Age. Since the rise of the Internet we have seen an evolving series of harms. At first, consumers faced distracting banner ads, pop-up ads, and spam.[374] Next, consumers faced behaviorally targeted ads that promised to be more relevant, yet also seemed more intrusive because of how intimately they suggested that marketers were mining our data.[375] The proliferation of Digital Age data collection and storage also led to increasingly common data breaches exposing vast stores of personal information.[376] Next, with the rise of predictive analytics, marketers made predictions about matters such as what social media content would make consumers click, whether to show specific consumers higher or lower prices, what levels of customer service to offer specific consumers, and even whether specific consumers are eligible for important benefits like employment, credit, housing, and insurance.[377] These same predictive tools allow political campaigns—and those who would undermine them—to target "fake news" and other messages intended to suppress one segment of the electorate or froth up another.[378] Online manipulation may be the newest tool in marketers' data-driven toolkit, but there will surely be more to come. Rather than attempting to regulate just one of those harms, I suggest using the threat of online

372. *See* Mik, *supra* note 331, at 24 ("The shift online challenges the assumption that consumers can detect and thus neutralise persuasive intent or information bias, not just because of the type but also the amount of influences."); EUROPEAN DATA PROTECTION SUPERVISOR, EDPS OPINION ON ONLINE MANIPULATION AND PERSONAL DATA 7 (2018), https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf ("Online manipulation may be viewed as the culmination of a three-stage cycle from data collection . . . through profiling to microtargeting or personalization as a form of manipulation which can vary in degree from trivial to seriously harmful.").

373. Calo, *supra* note 7, at 1003–18; Zarsky, *Privacy and Manipulation*, *supra* note 7, at 169; Susser et al., *supra* note 5, at 2.

374. WU, *supra* note 371, 189–90, 209; Bennett, *supra* note 112, at 900.

375. *See* WU, *supra* note 371, at 335–36; Bennett, *supra* note 112, at 900–01.

376. *See, e.g.*, Miles L. Galbraith, Comment, *Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, 62 AM. U. L. REV. 1365, 1372–73 (2013); Juliana DeGroot, *The History of Data Breaches*, DATA INSIDER (Oct. 24, 2019), https://digitalguardian.com/blog/history-data-breaches.

377. *See* Shaun B. Spencer, *Privacy and Predictive Analytics in E-Commerce*, 49 NEW ENGL. L. REV. 629, 633–38 (2015).

378. *See, e.*g., DIGITAL, CULTURE, MEDIA AND SPORT COMMITTEE, HOUSE OF COMMONS, DISINFORMATION AND "FAKE NEWS": FINAL REPORT, HC791 (Feb. 18, 2019), https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf; Janet Burns, *Whistleblower: Bannon Sought to Suppress Black Voters with Cambridge Analytica*, FORBES (May 19, 2018, 12:58 PM), https://www.forbes.com/sites/janetwburns/2018/05/19/cambridge-analytica-whistleblower-bannon-sought-to-suppress-black-voters/#7d347c517a95; Alex Hern, *Cambridge Analytica: How Did It Turn Clicks into Votes?*, GUARDIAN (May 6, 2018, 3:00 PM), https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie.

manipulation as another argument for comprehensive regulation of the data sharing ecosystem that makes all of the foregoing harms possible and facilitate future harms that we cannot yet imagine.[379]

Rather than pursue piecemeal solutions for each discrete harm, comprehensive data security legislation should adopt a systemic solution to reach the root causes of this ever-expanding list of harms. We have always been subjected in some form to unwanted sales pitches. And long before the Digital Age, data brokers were compiling consumer profiles from a wealth of private and public sources. But two features of the Digital Age have combined to magnify the potential harms to consumers. First, evolving data collection technologies allow marketers to build, store, and share unprecedented dossiers of our online and offline behaviors.[380] Second, evolving data analytics techniques allow marketers to operationalize these dossiers in real time, at the very moment when they are most able to influence a consumer's behavior or constrain a consumer's choices.[381]

Effective data protection legislation must constrain the steps in the data flow that lead most directly to the consumer harms while avoiding undue commercial disruption. One simple way to conceive of this data flow is a four-step process of collection, storage, sharing, and use.[382] A comprehensive data protecting regime could constrain some or all of these steps. First, legislation could constrain the collection of data itself.[383] After all, if no data can be collected, then there would be no data to build the dossiers used to target and manipulate consumers. Constraining collection, however, would prohibit marketers from many other uses of that data, such as analyzing the practices and preferences of their own consumers.

Next, legislation could constrain storage beyond the length of time necessary to complete the transaction or interaction. Such an approach could allow a narrow category of behavioral advertising tailored to the transaction or activity the consumer was engaged in at the moment,[384] while still prohibiting marketers

379. *Accord* Calo, *supra* note 7, at 1042–43 (suggesting that strengthening privacy protections will mitigate the digital market manipulation problem since digital market manipulation depends on information about consumers); Zarsky, *Online Privacy*, *supra* note 261, at 211–12 (proposing that, when consumers receive tailored advertisements, advertisers must provide notice that the content they are receiving is tailored to them). For other potential indirect regulation, see Calo, *supra* note 7, at 1047–48 (proposing that internet platforms be required to offer paid, marketing-free options); Kilovaty, *supra* note 8, at 465–68 (proposing that the potential harms necessary to trigger data breach laws include the risk of future manipulation flowing from a data breach).

380. Kilovaty, *supra* note 8, at 465.

381. *See id.* at 477.

382. Each of these steps may not happen in every case, and there are certainly more complex models of the data "life cycle." But this simple model will suffice for present purposes.

383. For each of these interventions, there would have to be exceptions that facilitate the practices necessary to accomplish the transaction or service the consumer has requested, and possibly exceptions strictly limited to troubleshooting the service provided and detecting fraud or malicious uses.

384. This approach, however, might not prevent manipulation based on real-time behaviors such as content typed, keystrokes, and facial expression. *See supra* text accompanying notes 172–77.

from leveraging insights gained from digital dossiers.[385] Like a collection constraint, however, a storage constraint would have far reaching impacts on how marketers understand their own customers.

Third, legislation could constrain sharing the information with third parties. This would prohibit most of the harmful practices discussed above that depend on real-time use of user profiles to target or manipulate consumers. This approach would still allow advertisers to employ traditional contextual advertising targeted at the audience likely to be visiting a particular web page.[386] In addition, a sharing constraint would help address concerns about data brokers building vast consumer profiles. One risk of this approach would be creating a potential advantage for major market players who have far more consumer data at their disposal than small players and new entrants.[387] Moreover, a very large player might have sufficient data on hand to create detailed dossiers and carry out real-time targeting, at least while consumers are interacting with that player.

Perhaps the most promising solution would be to target the use stage in ways that prohibit the automated processing necessary for real-time implementation of the analytics tools marketers need to decide what ad, offer, or message to target at particular consumers.[388] Such automated processing constraints would prohibit the worst of the harms identified above[389] and would avoid the sharing constraint's risk of allowing the biggest players to conduct behavioral

385. Allowing this limited form of behavioral targeting based on a user's current activities might in fact be an appropriate way to restore the balance between marketer and consumer. A consumer's actions might be used against her in the context of the present transaction, just as they could if the consumer walked into a retail store or car dealership where the salesperson observed her behaviors. But the consumer's aggregated behaviors would not follow her around to be used against her, just as a traditional salesperson could not follow the consumer and provide intelligence to the next salesperson.

386. When *The New York Times* terminated behavioral advertising on its European pages to avoid flooding users with consent requests required by GDPR, its revenue actually increased through reliance on contextual and geographic programming. Jessica Davies, *After GDPR, The New York Times Cut Off Ad Exchanges in Europe—and Kept Growing Ad Revenue*, DIGIDAY (Jan. 26, 2019), https://digiday.com/media/new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/. A subsequent study of forty publishers found that 45% of respondents reported that behavioral advertising "has not produced any notable benefit," and 23% reported that behavioral advertising "actually caused their ad revenues to decline." Mark Weiss, *Digiday Research: Most Publishers Don't Benefit From Behavioral Ad Targeting*, DIGIDAY (June 5, 2019), https://digiday.com/media/digiday-research-most-publishers-dont-benefit-from-behavioral-ad-targeting/.

387. Any constraint on sharing would have to address the potential "lookalike audiences" loophole, in which large data holders allow third-parties to deliver targeted messages to an audience with a specific data profile without actually sharing data with the third party. *See, e.g.*, *About Lookalike Audiences*, FACEBOOK.COM, https://www.facebook.com/business/help/164749007013531 (last visited Mar. 29, 2020).

388. *E.g.*, Council Regulation 2016/679, art. 22, 2016 O.J. (L 119) 1 (providing "right not to be subject to a decision based solely on automated processing, including profiling"); Council Regulation 2016/679, art. 4, 2016 O.J. (L 119) 1 (stating that "'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements").

389. If drafted broadly enough, automated processing constraints could also mitigate the problem of manipulation in political discourse and election debates, perhaps by holding data holders liable for ensuring that those with whom they share data comply with the automated processing constraints. *See, e.g.*, Data Care Act of 2018, S. 3744, 115th Cong. (2018) § 2(b)(3)(B) & (C) (prohibiting data holder from sharing data with third parties unless the sharer enters into a contract imposing the data holder's obligations of care and loyalty upon the third party, and requiring data holder to "take reasonable steps" to ensure compliance by the third party).

targeting based on their extensive customer data. Of course, an automated processing constraint might still grant large players an advantage in a world of purely contextual advertising because the bigger players will have the largest audiences. But that advantage has existed throughout the history of advertising-supported print and broadcast media. Such an approach would be a reasonable compromise because marketers could conduct contextual advertising while consumers could browse, shop, and share without fear that their behaviors will eventually be used against them. This approach might doom business models that exist purely to generate user data that can be monetized as part of the surveillance economy. Limiting the potential of such parasitic business models, however, might be another welcome benefit of a processing constraint.

After deciding what step or steps to constrain, legislators will then have to decide what form the constraint will take. Will it rely on the traditional notice and choice model, and if so, will that model take an opt-out[390] or opt-in[391] approach? Marketers heavily favor the notice and choice model, and in particular the opt-out approach.[392] But there is strong reason to believe that notice and choice can no longer protect consumer privacy, if indeed it ever could.[393] And

390. *E.g.*, Sen. Ron Wyden's Draft Consumer Data Protection Act § 6 (Nov. 1, 2018), https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy (providing opt-out consent via federal do-not-track registry); California Consumer Privacy Act of 2018, codified at CAL. LEGIS. CODE § 1798.120 (providing consumer right to opt out of data sharing).

391. *E.g.*, Council Regulation 2016/679, art. 4, 2016 O.J. (L 119) 1 (consent must be "freely given, specific, informed and unambiguous" and must be a "statement or clear affirmative action[ ] signif[ying] agreement"); Council Regulation 2016/679, art. 6, 2016 O.J. (L 119) 1 (imposing consent as one legal basis for data processing); Information Transparency & Personal Data Control Act, H.R. 6864, 115th Cong., §§ 1 & 4 (2018) (requiring opt-in consent for collection and use of "sensitive personal information" and opt-out consent for "non-sensitive personal information). The two-tiered approach of opt-in for sensitive information and opt-out for other information provides only an illusion of protection for the sensitive information. A marketer who secured opt-in consent from a subset of its users may use predictive analytics to discover what non-sensitive information is the best proxy for sensitive information. *See, e.g.*, Marianne Bertrand & Emir Kamenica, *Coming Apart? Cultural Distances in the United States Over Time* 10–13 (Nat'l Bureau of Econ. Research, Working Paper No. 24771, 2018), https://www.nber.org/papers/w24771.pdf (describing machine learning model that uses data on "time use, social attitudes, media consumption, and consumer behavior" to predict "income, education, gender, race, and political ideology"); Tobias Berg et al., *On the Rise of Fintechs—Credit Scoring Using Digital Fingerprints* 2–3 (Nat'l Bureau of Econ. Research, Working Paper No. 24551, 2018), https://www.nber.org/papers/w24551.pdf (predicting creditworthiness using "digital footprint" information gathered from the mere act of visiting a webpage, without any need for sharing text, financial information, or social network data).

392. Lauren E. Willis, *Why Not Privacy by Default?*, 29 BERKELEY TECH. L.J. 61, 67–68 (2014) (firms favor opt-out default).

393. *Policy Principles for a Federal Data Privacy Framework in the United States: Hearing Before the S. Comm. On Commerce, Science, & Transportation*, 116th Cong. 5 (2019) (Statement of Woodrow Hartzog, Professor of Law and Computer Science, Northeastern University), https://www.commerce.senate.gov/services/files/8B9ADFCC-89E6-4DF3-9471-5FD287051B53 (arguing that notice and choice is ineffective in the Digital Age); *Protecting Consumer Privacy in the Era of Big Data, Hearing Before the H. Comm. On Energy & Commerce, Subcomm. On Consumer Protection & Commerce*, 116th Cong., (2019) (statement of Nuala O'Connor, President and CEO, Center for Democracy & Technology), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony_Nuala%20O%27Connor%2002.26.2019.pdf; Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880–81 (2013); Woodrow Hartzog, *The Inadequate, Inalienable Fair Information Practices*, 76 MARYLAND L. REV. 952, 974–75 (2017); Lisa M. Austin, *Enough About Me: Why Privacy Is About Power, Not Consent (or Harm)*, *in* A WORD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO? 131, 132–33, 189 (Austin Sarat ed. 2015).

even if the legislation took an opt-in approach, marketers are skilled at drafting opt-in requests in ways that manipulate consumers into giving that consent.[394] The more promising approach, then, would be to establish duties or prohibitions that exist regardless of consent.[395]

Finally, using the threat of online manipulation to support comprehensive data protection legislation offers several practical benefits. First, the push for data protection legislation is gaining momentum in a way that we have not seen for decades. Given that momentum, such legislation might be more likely to pass than legislation targeted at just one type of data-driven influence tool. Second, given the stark nature of the threat that online manipulation poses, adding online manipulation to the list of potential data harms may increase support for comprehensive data protection legislation. Third, given the amount of political bandwidth that the broader data protection debate currently occupies, it seems unlikely that a separate push to regulate online manipulation would gain sufficient traction. Fourth, as discussed above, any effort to regulate online manipulation directly poses difficult definitional questions that would likely bog down, or at least water down, any regulation that might pass. Finally, a comprehensive data protection law will be better positioned to withstand First Amendment scrutiny than a law directly regulating online manipulation. In sum, the best way to solve the online manipulation problem is to treat it as one piece of the larger data protection puzzle.

394. *See, e.g.*, Statement of Woodrow Hartzog, *supra* note 393 (describing how data collectors "leverage design to extract our consent").

395. *E.g.*, Data Care Act of 2018, S. 3744, 115th Cong. (2018) § 3 (imposing duties of care, loyalty, and confidentiality, with no exception for consent).