UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 23 | Issue 3 Article 2

4-1-2022

Manipulation, Privacy, And Choice

Kirsten Martin

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 23, ISSUE 3: APRIL 2022

MANIPULATION, PRIVACY, AND CHOICE

Kirsten Martin*

As individuals navigate their lives on websites and apps, their movements, searches, and actions are silently tracked. Streams of consumer data are then pooled by data aggregators and mined to identify potential vulnerabilities of consumers. These potential weaknesses, e.g., whether someone is in financial distress, having a health crisis, or battling an addiction, are valuable to marketers and ad networks to silently steer consumers' market actions towards the manipulator's interests. While identified early on as problematic within the economics of information broadly, the use of hyper-targeting to manipulate consumers is underappreciated as a threat to not only the autonomy of individuals but also the efficiency and legitimacy of markets.

This Article examines targeted manipulation as the covert leveraging of a specific target's vulnerabilities to steer their decisions to the manipulator's interests. This Article positions online targeted manipulation as undermining the core economic assumptions of authentic choice in the market. Then, this Article explores how important choice is to markets and economics, how firms gained positions of power to exploit vulnerabilities and weaknesses of individuals without the requisite safeguards in place, and how to govern firms that are in the position to manipulate. The power to manipulate is the power to undermine choice in the market. As such, firms in the position to manipulate threaten the autonomy of individuals, diminish the efficiency of transactions, and undermine the legitimacy of markets.

* Kirsten Martin, PhD is the William P. and Hazel B. White Center Professor of Technology Ethics at *University of Notre Dame's* Mendoza College of Business. kmarti33@nd.edu. I wish to thank Alessandro Acquisti, Ryan Calo, Shaun Spencer, Daniel Susser, Ari Walman, Tal Zarsky as well as the participants of the 2019 Northeastern Privacy Scholars Conference for their helpful comments on an earlier version of this argument.

This Article argues that firms merely in the position to manipulate, with knowledge of individual's weaknesses and access to their decision-making, should be regulated to ensure those firms' interests are aligned with the target. The economic oddity is not that firms have data that render another market actor vulnerable, but rather the oddity is that so many firms have data to covertly manipulate others without safeguards in place. Market actors regularly share information about their concerns, preferences, weaknesses, and strengths within contracts or joint ventures or within a relationship with professional duties.

The point of manipulation is to covertly steer a target's decision towards the manipulator's interests and away from the target's; as such, manipulation impedes a market actor's ability to enact preferences through choice. This undermining of choice—and not the harming of consumers—is the basis for additional safeguards on those in the position to manipulate. Governing targeted manipulation online will require additional safeguards on those firms in the position manipulate rather than attempting to identify each instance of targeted manipulation. First, additional safeguards are needed to limit data aggregators and ad networks—specifically, any data trafficker without any relationship with consumers—to ensure the use of information is in the interests of the consumer. Second, consumer-facing websites and apps act as gatekeepers by luring in consumers to have their data tracked by third parties and later to be targeted with manipulative content. In so doing, consumer-facing companies should be responsible for ensuring all third parties that access their users—either for data collection or for targeting content—abide by standards of care that are audited. Where scholarship has focused on identifying instances of manipulation to regulate, this Article argues that firms merely in the position to manipulate, with knowledge of the individual and access to their decision-making, should be regulated to ensure their interests are aligned with the target.

TABLE OF CONTENTS

"One should hardly have to tell academicians that information is a valuable resource: knowledge is power."[1]

For online marketing, "data giant Acxiom provided up to 3,000 attributes on 700 million people [including purchases, net worth, number of children, and health interests] . . . [one year later] the number was 10,000, on 2.5 billion consumers."[2]

I. INTRODUCTION

Data brokers proudly collect information on millions of individuals with thousands of data points on each individual, or "target."[3] These companies collect this information from, among other sources, browsing history, shopping, location tracking, and public records, and can use this mundane information to predict, for example, if someone is depressed, anorexic, addicted to drugs or alcohol, or has a medical condition.[4] Ad networks and advertisers are willing to pay top dollar to identify those in financial and emotional difficulty to promote gambling, cures, rehab, and payday loans, and to more effectively target vulnerable consumers generally.[5] As Professor Paul Ohm succinctly summarizes,

---

[1] George J. Stigler, *The Economics of Information*, 69 J. POL. ECON. 213, 213 (1961).

[2] Steve Melendez & Alex Pasternack, *Here are the data brokers quietly buying and selling your personal information*, FAST CO. (Mar. 2, 2019), https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information [https://perma.cc/P6UK-AFCB].

[3] *See* Melendez & Pasternack, *supra* note 2.

[4] *See generally* Kirsten Martin & Helen Nissenbaum, *What is it about Location?*, 35 BERK. TECH. L.J. 251 (2020); Kirsten Martin & Helen Nissenbaum, *Privacy Interests in Public Records: An Empirical Investigation*, 31 HARV. J.L. & TECH. 111 (2017) [hereinafter Martin & Nissenbaum, *Privacy Interests in Public Records: An Empirical Investigation*]; Kashmir Hill, *Data Broker Was Selling Lists Of Rape Victims, Alcoholics, and 'Erectile Dysfunction Sufferer*, FORBES (Dec. 19, 2013), https://www.forbes.com/sites/kashmirhill/2013/12/19/data-broker-was-selling-lists-of-rape-alcoholism-and-erectile-dysfunction-sufferers/?sh=3d72b8861d53 [https://perma.cc/4LXS-54W3]; *What Information Do Data Brokers Have on Consumers, and How Do They Use It?: Hearing Before the S. Comm. on Com., Sci., and Transp.*, 113th Cong. (2013).

[5] *See* Elisa Gabbert, *The 25 Most Expensive Keywords in Google Ads*, WORDSTREAM (June 27, 2017), https://www.wordstream.com/blog/ws/2017/

"[companies] hoard this data for future, undefined uses; redistribute it to countless third parties; and repurpose it in ways their customers never imagined."[6]

Advances in hyper-targeted marketing allow firms to generate leads, tailor search results, place content, and develop advertising based on a detailed picture of their target.[7] This Article calls such tactics "targeted manipulation," which is the covert leveraging about a specific target's vulnerabilities to steer their decision to the manipulator's interest. As Professor Ryan Calo predicted in one of the first papers on the manipulation of online consumers, hyper-targeting, combined with the data collected on individuals, can allow firms to, for example, predict moods, personality, stress levels, health issues, etc., and potentially use that information to undermine the decisions of consumers.[8] In fact, Facebook offered advertisers the ability to target teens who are "psychologically vulnerable."[9] Data aggregators, data brokers, ad networks, and other

---

06/27/most-expensive-keywords [https://perma.cc/RK37-Y9Y9]. Examples of keywords related to urgent problems were ranked by how much marketers were willing to pay for them and included: "Bail bonds" at #2, "Lawyer" at #4, "Cash services & payday loans" at #7, "Rehab" at #11, "Plumber" at #18, "Termites" at #19, and "Pest control" at #20. *Id.*

[6] Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1128 (2015) (citing Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J.: WHAT THEY KNOW SERIES (July 30, 2010), http://online.wsj.com/news/articles/SB10001424052748703940904575395073512989404 [https://perma.cc/8WEM-RZBC]).

[7] As an example, companies can morph a target's face with a model for advertising. Such face-morphs are thought to be more trusting than a stranger; however, initial experiments have not shown this increased trust to impact behavior. Sonam Samat, Eyal Peer & Alessandro Acquisti, *Can Digital Face-Morphs Influence Attitudes and Online Behaviors?*, PROC. FOURTEENTH SYMP. 117, 117 (2018) ("Thus, self-morphs may be used online as covert forms of targeted marketing – for instance, using consumers' pictures from social media streams to create self-morphs, and inserting the resulting self-morphs in promotional campaigns targeted at those consumers.").

[8] *See* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 996 (2014). *See generally* TAL Z. ZARSKY, *Online Privacy, Tailoring, and Persuasion*, *in* PRIVACY & TECHNOLOGIES OF IDENTITY 209 (2006).

[9] 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/ [https://perma.cc/APW6-7KXS].

types of "data traffickers"[10] can not only predict what consumers want and how badly they need it, but can also leverage knowledge about individuals' vulnerabilities to steer their decisions in the interest of the firm.[11]

Recent examinations of online consumer manipulation have either defined manipulation broadly to include standard persuasion and advertising tactics,[12] or have focused on the use of human psychology to prime market decisions across consumers (e.g., nudging or dark patterns).[13] Folding targeted manipulation within persuasion or nudging allows manipulation—which operates closer to fraud or coercion in undermining choice in the market—to hide within more innocuous or difficult-to-regulate tactics that are deployed broadly across a group of users.

The phenomenon of interest is the ability of firms to covertly leverage a target's vulnerabilities to steer their decision towards the manipulator's interests. In doing so, this Article moves away from broader interpretations of manipulation that are centered on irrational decisions, nudges, and persuasion, which all render

---

[10] Professor Lauren Scholz uses the term "data traffickers" to include companies that traffic in consumer data behind the scenes and without the knowledge of the consumer. *See* Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L. J. 653, 664–67 (2019). This Author uses this term throughout this Article to mean any company with individualized data without a relationship with users or customers. These companies make their money trafficking consumer data. *Id.*

[11] *See, e.g.*, Calo, *supra* note 8, at 996; *see also* ZARSKY, *supra* note 8, at 209.

[12] *See, e.g.*, Cass R. Sunstein, *Fifty Shades of Manipulation*, 1 J. MKTG. BEHAV. 213, 213 (2016).

[13] "Nudging" is the use of user interfaces to steer users to a preferred outcome, while dark patterns is the use of user interfaces for the benefit of the company. *See* Shmuel I. Becher & Yuval Feldman, *Manipulating, Fast and Slow: The Law of Non-Verbal Market Manipulations*, 38 CARDOZO L. REV. 459, 459 (2016); T. Martin Wilkinson, *Nudging and Manipulation*, 61 POL. STUD. 341, 341 (2013); Anne Barnhill, *I'd like to Teach the World to Think: Commercial Advertising and Manipulation*, 1 J. MKTG. BEHAV. 307, 307 (2016); Arvind Narayanan et al., *Dark Patterns: Past, Present, and Future*, 18 QUEUE 67, 67 (2020); Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'*, 31 CURRENT OP. PSYCH. 105, 105 (2020). *See also* Alessandro Acquisti et al., *Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online*, 50 ACM COMPUTING SURV. (CSUR) 1, 1 (2017) (summarizing the research on nudges regarding privacy).

manipulation so pervasive as to be un-governable.[14] Instead, this Article focuses on a stricter conceptualization—well known within law, philosophy, and economics—that focuses on the hidden nature of the tactic to exploit a specific target's vulnerabilities in order to hijack their decisions to the manipulator's ends.[15] Targeted manipulation defined here has three important factors: (1) the exploitation of an individual's vulnerabilities; (2) the covertness of the tactic; and, (3) the divergence of interests between the manipulator and the target.

More specifically, this conceptualization focuses on manipulation as undermining an individual's ability to enact their preferences through choice. Individuals generally seek to preserve choice in the market, where consumer choice is meaningful and indicative of consent to the transaction.[16] Preserving choice-as-an-indicator-of-consent is not only critical for autonomy and for a robust political society, but is also a fundamental assumption in economics and business as to the efficiency of transactions and the legitimacy of markets.[17] As such, this Article positions manipulation as a close cousin to coercion and fraud in undermining an individual's choice in the market. Positioning targeted manipulation as akin to coercion and fraud changes the conversation about governance and brings in new parallel examples offline where consumer choice is protected.[18]

Accordingly, this Article argues that firms *merely in the position* to manipulate, with knowledge of individuals and access to individuals' decision-making, should be regulated to ensure firms' interests are aligned with the target individual. In other areas, when someone is in a position to manipulate an individual—in a position to exploit the relative vulnerabilities or weaknesses of a target in

---

[14] *See, e.g.*, Sunstein, *supra* note 12.

[15] *See* Daniel Susser, Beate Roessler & and Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1, 3 (2019); JOSEPH RAZ, THE MORALITY OF FREEDOM 378 (1988); Eric A. Posner, *The Law, Economics, and Psychology of Manipulation*, 1 J. MKTG. BEHAV. 267, 267 (2016).

[16] *See infra* Part III.A.

[17] *See id.*

[18] *See id.*

order to usurp their decision-making—safeguards force their interests to be aligned and punish acts that are seen as out of alignment with the target.[19] Given this odd economic situation, where data traffickers have the knowledge and proximity of an intimate relationship, without the governance and trust inherent to such relationships in the market, the question becomes: *How did firms gain positions of power to exploit vulnerabilities and weaknesses of individuals without the requisite safeguards in place?* This Article argues that this current market problem—where firms, whose interests do not align with consumers, have the knowledge and position to manipulate consumers—arises from the incorrect framing of privacy as relinquished upon disclosure in economics and law.[20]

Governing targeted manipulation online will require placing responsibility on those in the position to manipulate rather than attempting to identify each instance of targeted manipulation. This Article advances two solutions in Part V below. First, external auditing of data aggregators and ad networks in the position to manipulate, with the individualized data to identify weaknesses and vulnerabilities of consumers, would ensure that the use of information is not used to manipulate consumers. This external auditing would entail data integrity principles that are enforced through auditing by third parties. Importantly, these duties do not rely on any harm to be quantified, an established consumer

---

[19] *See infra* Part III. B.

[20] This Article does not cover the harm suffered by the individual being surveilled in the vast collection of consumer data. Not further discussing such harm is not meant to diminish the ethical implications of surveillance, only to narrow the scope of the article. For example, respondents find that being surveilled while forming preferences undermines their autonomy. *See* Yonat Zwebner & Rom Y. Schrift, *On My Own: The Aversion to Being Observed During the Preference-Construction Stage*, 47 J. CONSUMER RSCH. 475, 475 (2020); Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, U. CHI. L. REV. 181, 181 (2008); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1373 (2000); Julie E. Cohen, *Turning Privacy inside Out*, 20 THEORETICAL INQUIRIES L. 1, 1 (2019). Professor Neil Richards defends intellectual privacy as the ability to develop ideas and beliefs away from an unwanted gaze. Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 389 (2008).

relationship, or any enforcement by consumers. Instead, this Article posits that data traffickers (i.e., companies that collect, store, and process individualized data) would be subject to annual audits similar to other industries that require public trust but are not otherwise regulated by the market (e.g., financing in banks, accounting in firms, environmental impact in manufacturing).[21]

Second, this Article argues that consumer-facing companies should be responsible for the third parties that access their users' information—either for the collection of data or for the targeting of content—and ensure that these third parties abide by standards of care and are audited. Consumer-facing websites and apps that lure consumers, so that consumers' data are collected and later used against them, should be held responsible for the third parties they invite to track and target their users. Current solutions place a duty of care or loyalty on consumer-facing firms, which can create pressure for these firms to then outsource bad privacy practices to third parties.[22] This Article offers a complementary solution to those arguing for duties of loyalty and care to be imposed on consumer-facing firms by (1) extending their duties to include a responsibility for the third parties that firms invite to track and target their users, and (2) placing additional safeguards, like auditing, on data traffickers that are in a position to manipulate consumers but are outside the reach of current regulations and proposed legal solutions, as well as outside market pressures.

This Article starts in Part II with an examination of targeted manipulation, comparing manipulation with related concepts ubiquitous in the market, such as nudges and price discrimination,

---

[21] *See* 12 C.F.R. § 363 (2022); 15 U.S.C. § 78q; 15 U.S.C. 2607(a).

[22] *See* Ian R. Kerr, *The Legal Relationship Between Online Service Providers and Users*, 35 CAN. BUS. L.J. 419, 427–28 (2001); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1185–86 (2016); Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 1 (2018); Neil M. Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 431 (2016) [hereinafter Richards & Hartzog, *Taking Trust Seriously in Privacy Law*]; Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. (forthcoming 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217 [https://perma.cc/75UK-3XKJ]) [hereinafter Richards & Hartzog, *A Duty of Loyalty for Privacy Law*].

as well as concepts banned in the market, such as fraud and coercion. In Part III, this Article positions online targeted manipulation as an economic abnormality in the market, which undermines the core economic assumptions of authentic choice. In Part IV, this Article explains how firms gained their positions of power and knowledge to exploit vulnerabilities and weaknesses of individuals without the requisite safeguards in place. This Article further argues that firms being in a position to leverage aggregated consumer data is a symptom of the mistaken framing of privacy-as-concealment in law, economics, and public policy. In Part V, this Article moves away from seeking to identify and regulate unique instances of manipulation, and instead argues that firms merely in a position to manipulate, with the knowledge of an individual's vulnerabilities and access to their decision-making, should be regulated to ensure the firm's interests are aligned with the target.

II. MANIPULATION AND THE PHENOMENON OF INTEREST

Targeted manipulation sits within a family of tactics whereby one actor attempts to exert influence over another. Therefore, delineating the boundaries of these concepts is critical to understand how and why targeted manipulation differs and is normally regulated. Subpart A explains the phenomenon of interest. Subpart B then outlines the necessary components of manipulation and differentiates targeted manipulation from related concepts, such as persuasion, nudges, fraud, and coercion. Finally, Subpart C examines how targeted manipulation is normally treated within economics regarding consumers and markets.

A. Phenomenon of Interest

The focus of this Article is targeted manipulation: the ability of firms with knowledge about individuals to leverage a specific target's vulnerabilities in order to covertly undermine their decision away from the interests of the consumer and towards the interests of the firm.[23] These vulnerabilities are identified through the broad collection of data across websites, apps, and technologies and then

[23] Targeted manipulation requires both the knowledge of the individual and the closeness to the decision-making. Offline, this is usually the same actor.

through collecting search terms, contacts, locations, and browsing histories.[24] Such "surface data" can be used to "infer latent, far more sensitive data about" individuals through predictive analytics.[25] As Professor Ryan Calo summarizes:

> [T]he consumer is shedding information that, without her knowledge or against her wishes, will be used to charge her as much as possible, to sell her a product or service she does not need or needs less of, or to convince her in a way that she would find objectionable were she aware of the practice.[26]

The knowledge of individuals' vulnerabilities can be tracked directly—through search queries for gambling, medical symptoms, or teenage depression, for example—or via inferences drawn from vast surface data, almost always when the consumer is not aware.[27] Firms now have access to data that can "predict mood, personality, stress levels, gender, marital and job status, age, level of disease, mental health issues, sleep, [and] physical movement,"[28] which can facilitate dynamic emotional targeting or psychographic targeting.[29]

---

[24] *See* Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 MD. L. REV. 439, 445 (2020).

[25] *Id.* at 439. As Ohm and Peppet note, everything can reveal everything. Paul Ohm & Scott Peppet, *What If Everything Reveals Everything?*, *in* BIG DATA IS NOT A MONOLITH, 45, 45 (MIT Press, 2016).

[26] Calo, *supra* note 8, at 1030.

[27] *See* Hirsch, *supra* note 24, at 441–42.

[28] Shaun B. Spencer, *The Problem of Online Manipulation*, 2020 U. ILL. L. REV. 959, 979 (2020). For example, IBM has filed a patent for a process that "help[s] 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." Sidney Fussell, *Alexa Wants to Know How You're Feeling Today*, ATLANTIC (Oct. 12, 2018), https://www.theatlantic.com/technology/archive/2018/10/alexa-emotion-detection-ai-surveillance/572884/ [https://perma.cc/49LN-RRDT].

[29] *See* Jacquelyn Burkell & Priscilla M. Regan, *Voter Preferences, Voter Manipulation, Voter Analytics: Policy Options for Less Surveillance and More Autonomy*, 8 INTERNET POL'Y REV. 1, 8 (2019). Burkell and Regan provide an excellent example leveraging the morphing of two faces (one being the target) into one person used in advertising. *Id.* at 4–5. Such tactics are used in commercial and political advertising. *See id.*; Daniel Susser et al. *Technology, Autonomy, and Manipulation*, 8 INTERNET POL'Y REV. 1, 2 (2019); Calo, *supra* note 8, at 997; Ira

Targeted manipulation is fueled by both this knowledge of individuals' vulnerabilities and by the individualized reach of hyper-targeted marketing. Ad networks and data traffickers are able to target specific individuals and therefore leverage individualized knowledge to undermine a consumer's decision-making.[30] In other words, targeting a consumer based on broad demographics (such as being a fifty-year-old male) is not as useful or specific as targeting an individual for being someone who is generally anxious and whose second child is heading to college in California. For example, the 2016 United States presidential campaigns relied on very specific ads viewed by only individuals who may have been swayed by them and not seen by individuals who may have been able to recognize the ads' inaccuracies.[31] Manipulation "affect[s] a person's

---

S. Rubinstein, *Voter Privacy in the Age of Big Data*, 2014 WIS. L. REV. 861, 861 (2014); Frederik J. Zuiderveen Borgesius et al., *Online Political Microtargeting: Promises and Threats for Democracy*, 14 UTRECHT L. REV. 82, 82 (2018). However, there may be limits as to the effectiveness at the individual level given current abilities. *See* Peer et al., *supra* note 7, at 117.

[30] The technique of hypertargeting, where an individual or small group of similar individuals are targeted, also ensures that hypertargeting is not seen by others who may not be susceptible to manipulation. In other words, hypertargeting not only supports the individualization of the manipulation and the ability to leverage specific vulnerabilities of a target against them, but also supports the manipulation being hidden from others. For example, manipulative advertising around the presidential election was so targeted on social network sites that no one aside from the target was able to see the advertising. Sathvik Tantry, *Making Personalized Marketing Work*, HARV. BUS. REV. (Feb. 29, 2016), https://hbr.org/2016/02/making-personalized-marketing-work [https://perma.cc/3S8H-45ZL]; *see also* Leslie K. John, Tami Kim & Kate Barasz, *Ads That Don't Overstep*, HARV. BUS. REV. (2018), https://hbr.org/2018/01/ads-that-dont-overstep [https://perma.cc/XJ33-LZF7].

[31] Issie Lapowsky, *How Russian Facebook Ads Divided and Targeted US Voters Before the 2016 Election*, WIRED (Apr. 16, 2018, 9:00 AM), https://www.wired.com/story/russian-facebook-ads-targeted-us-voters-before-2016-election/ [https://perma.cc/FDR2-RSAK]. *See* S. SELECT COMM. ON INTEL., 116TH CONG., REP. ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION VOLUME 2: RUSSIA'S USE OF SOCIAL MEDIA WITH ADDITIONAL VIEWS (2016).

thoughts, opinions, and actions" and is designed to exploit specific vulnerabilities of the target.[32]

Previous examinations have pooled together targeted manipulation with broader attempts to steer consumers and users, such as the use of dark patterns and nudges.[33] This is not to say that dark patterns and nudges are not important to examine, only that the specific problems with targeted manipulation, i.e., the gathering and use of information about individuals and the reach to undermine specific targets' decisions, get lost in a larger examination of broader tactics.[34] This Article remains focused on the phenomenon of interest—targeted manipulation online—and does not examine broader attempts to change behavior online, such as with nudges and dark patterns. [35]

---

[32] "Internet actors, political entities, and foreign adversaries carefully study the personality traits and vulnerabilities of Internet users and, increasingly, target each such user with an individually tailored stream of information or misinformation with the intent of exploiting the weaknesses of these individuals." Ido Kilovaty*, Legally Cognizable Manipulation*, 34 BERKELEY TECH. L.J. 449, 464 (2019).

[33] *See* Acquisti et al., *supra* note 13; Arunesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 81 PROC. ACM HUMAN-COMPUTER INTERACTION 1, 3 (2019); Narayanan et al., *supra* note 13; Waldman, *supra* note 13; Cass R. Sunstein, *Nudges Do Not Undermine Human Agency*, 38 J. CONSUMER POL'Y 207, 207 (2015). As a caveat to this statement, nudges and dark patterns that are based on individualized vulnerabilities and target a specific individual would be included in this analysis and would be closer to targeted manipulation as such. For example, Professors Warberg, Acquisti, and Sicker test the efficacy of tailoring a nudge to a specific psychometric measurement; that type of targeting was not effective in impacting disclosure. *See* Logan Warberg, Alessandro Acquisti & Douglas Sicker, *Can Privacy Nudges Be Tailored to Individuals' Decision Making and Personality Traits?*, PROC. 18TH ACM WORKSHOP PRIV. ELEC. SOC. 175, 175 (2019).

[34] This Article also does not explicitly cover the issues around gamification or addictive designs, which are also important attempts to modify consumer behavior broadly. *See* Tae Wan Kim & Kevin Werbach, *More than Just a Game: Ethical Issues in Gamification*, 18 ETHICS & INFO. TECH. 157, 157 (2016).

[35] This assertion is picking up the first argument of Ryan Calo's seminal article, *Digital Market Manipulation*, Calo, *supra* note 8, which is "that the digitization of commerce dramatically alters the capacity of firms to influence consumers at a personal level." Calo, *supra* note 8, at 999. Professor Calo goes on to also include

B. Necessary Components of Manipulation

Targeted manipulation is defined here as leveraging the vulnerabilities of individuals in order to covertly steer a target's decision towards the interests of the manipulator. Offline, threats of manipulation are usually associated with established relationships where the manipulator knows the vulnerabilities and weaknesses of the target and is in a position to covertly undermine the target's decision. For example, a financial advisor or lawyer would know the vulnerabilities of a client due to the intimate knowledge provided within the relationship and could, if not against professional obligations, use that information to steer the target's decision towards the advisor's or lawyer's interests. Similarly, a caregiver would know the vulnerabilities of their charge (a toddler, a patient, etc.) and would be close enough to be able to manipulate their decisions away from the interest of the charge and towards the interest of the caregiver.

Thus, targeted manipulation[36] has three important factors: (1) the exploitation of an individual's vulnerabilities; (2) the covertness of tactic; and, (3) the divergence of interests between manipulator and target. This Article explores each below and explains why each factor distinguishes this examination from previous work on online manipulation.

1. Exploitation of an Individual's Vulnerabilities

Key to manipulation is leveraging an individual's weaknesses or vulnerabilities in order to subvert the target's decision-making. While other tactics seek to undermine decision-making in the market (e.g., fraud, coercion, opportunism, etc.), manipulation uniquely uses a target's vulnerabilities as the tool to subvert decision-making. A common example is the manipulation of children, which is usually performed by parents and teachers, who

---

broader attempts to sway decisions online, such as the use of biases and nudges. *Id.* at 1007–12. However, this Article will remain focused on the targeted manipulation he first brought up. *Id.*

[36] Targeted manipulation is defined here as leveraging the vulnerabilities of individuals in order to covertly steer a target's decision towards the interests of the manipulator. The three factors correspond to the three components of the definition.

take advantage of their targets' lack of knowledge and lack of experience. But manipulation can also be based on a firm's relative position of power and unique knowledge about the target.

As first identified by Professor Ryan Calo, online firms are able to identify ego depletion of consumers—where they are vulnerable and easily manipulated—based on detailed profiles of consumers.[37] These companies collect "surface data"[38] to predict if someone is depressed, anorexic, addicted to drugs or alcohol, or has a medical condition, and then those companies link that information to the person's location, what decisions the person may be making, and where the person may go next.[39] Ad networks and advertisers use this information and are willing to pay these companies top dollar to identify people in financial and emotional distress to promote gambling, cures, rehab, and payday loans, for example.[40]

Firms, platforms, and other data aggregators are also in a structural position of power over their users because these data collectors retain the unique services and knowledge individuals are seeking, and the data aggregators create an information asymmetry by preventing their users from fully understanding how their data is

---

[37] Calo's focus was more general than what is examined here: the ability to influence consumers by exploiting their tendency to act with biases or act "irrationally." *See* Calo, *supra* note 8, at 1010.

[38] Hirsch notes that the more innocuous data individuals shed when online (e.g., like the purchase of furniture anti-scuff pads) can be analyzed with predictive analytics to identify latent knowledge ("like credit card default risk"). Hirsch, *supra* note 24, at 456. "[P]redictive analytics takes surface data and infers latent information from it. This makes it difficult, if not impossible, for people to know what they are really sharing when they agree to disclose their surface data." *Id.* at 442.

[39] Yonat Zwebner & Rom Y. Schrift, *On My Own: The Aversion to Being Observed during the Preference-Construction Stage*, 47 J. CONSUMER RES. 475, 476 (2020).

[40] *See* Gabbert, *supra* note 5 (ranking the keywords related to urgent problems in Google Ads in order from most expensive to least; examples include: "bail bonds" ranked 2nd most expensive, "lawyer" ranked 4th most expensive, "cash services & payday loans" ranked 7th most expensive, "rehab" ranked 11th most expensive, "plumber" ranked 18th most expensive, "termites" ranked 19th most expensive, and "pest control" ranked 20th most expensive).

used and leveraged.[41] Thus, individuals are in a position of vulnerability vis-à-vis the data controller.[42] While anyone can deceive or commit fraud, manipulation requires a power or knowledge imbalance rendering the target vulnerable to exploitation. The target can be in a perennial vulnerable state (such as a child with an adult); or, the target can be in a temporary vulnerable state (such as when a client provides details to a lawyer or therapist, or when a company provides concerns, preferences, and forecasts to a third party).[43]

2. Covertness of Tactic

Manipulation works because it is covert and hidden from the target. In other words, the target must be unaware of the tactic being used for manipulation to be effective. According to scholars Daniel Susser, Beate Roessler, and Helen Nissenbaum:

> [M]anipulative practices often work by targeting and exploiting our decision-making vulnerabilities—concealing their effects, leaving us unaware of the influence on our decision-making process—they also challenge our capacity to reflect on and endorse our reasons for acting as authentically on our own. Online manipulation thus harms us both by inducing us to act *toward ends* not of our choosing and *for reasons* we haven't endorsed.[44]

This hiddenness is important because, first, it suggests an intention to hijack a decision without regard to the target's interests; otherwise, more overt arguments and persuasion would be used. Covertness in manipulation is necessary because the target would likely never endorse the tactic if the target were aware of the

---

[41] Kirsten Martin, *Transaction Costs, Privacy, and Trust: The Laudable Goals and Ultimate Failure of Notice and Choice to Respect Privacy Online*, 18 FIRST MONDAY (Dec. 2013), https://firstmonday.org/ojs/index.php/fm/article/view/4838/3802 [https://perma.cc/YH3H-YXTH].

[42] Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 497 (2019).

[43] These concerns, preferences, and projections can be constructed from the target's lived experiences and are constantly evolving.

[44] Susser, Roessler & Nissenbaum, *supra* note 29, at 10; *see also* Alan Ware, *The Concept of Manipulation: Its Relation to Democracy and Power*, 11 BRIT. J. POL. SCI. 163, 165 (1981) (considering when A has manipulated B, "B either has no knowledge of, or does not understand, the ways in which A affects his choices").

attempted manipulation. Second, hiddenness also renders the manipulation harder to combat, identify, and regulate. In fact, hiddenness is so central to manipulation that Professor Ryan Calo suggests disclosure would minimize the harm or power of manipulation: If "manipulation subjects are informed, the potency of manipulation may be weakened."[45] For example, imagine if the target was told, "We are marketing this product to you because we think you are a diabetic and particularly tired right now." The target would probably be outraged, insulted, and more easily able to walk away from or counter the manipulation.

Hiddenness also differentiates manipulation from mere persuasion.[46] Persuasion engages in the marketplace of ideas by being open and subject to counter arguments.[47] Conversely, targeted manipulation circumvents the marketplace of ideas by being hidden. Persuasion works because the tactic is known by the target, whereas manipulation works only if the tactic is hidden.[48] In fact, manipulation is necessary when direct, open appeals to the preferences of the target fail.[49] For instance, one can attempt to persuade a child to put on clothes or a consumer to buy a soft drink by openly engaging with the target using cogent (or not so cogent) arguments. In this way, manipulation starts where persuasion

---

[45] Kilovaty, *supra* note 32, at 462.

[46] Zarsky presents an alternative view: Manipulation is just unseemly persuasion, defined as "a process in which firms strive to motivate and influence individuals to take specific steps and make particular decisions in a manner considered to be socially unacceptable." Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRIES L. 157, 158 (2019). He notes that this is a broad issue, stating, "[s]triving to manipulate and exert influence is, of course, not new. Quite to the contrary, almost every form of human communication tries to do so." *Id.* at 170. *See also* Barnhill, *supra* note 13, at 307 (using examples such as nudging or priming, as well as simple print advertising and persuasion in the analysis of manipulation). By broadening the phenomenon of interest to include persuasion (Zarsky) and nudges (Barnhill), the problematic tactic of targeted manipulation can hide amongst the less problematic and harder to govern tactics of nudges and persuasion.

[47] One cannot counter manipulation with more speech—because manipulation is an attempt to circumvent the marketplace of ideas by not using up front persuasion.

[48] *See* Barnhill, *supra* note 13.

[49] *See id.*

ends—where the manipulator ceases to engage openly with the target in a way that affords the target the ability to counter.

Conflating manipulation with persuasion makes the threat of manipulation seem harmless and omnipresent. Professor Cass Sunstein defines manipulation as a form of persuasion, arguing that "the problem is that . . . manipulation can plausibly be said to be pervasive. It can be found on television, on the Internet, in every political campaign, in countless markets, in friendships, and in family life."[50] Defenders of manipulation in economics, marketing, or practice have broadened the definition to include persuasion and advertising, thereby rendering the definition of manipulation so broad as to include legitimate acts—effectively making the deceptive act impossible to regulate.[51]

3. Divergence of Interests Between Manipulator and Target

Finally, the goal of manipulation is to prevent targets from pursuing their own interests and to "promote the outcome sought by the manipulator."[52] Parents who manipulate their toddler to get dressed before going outside are attempting to usurp the child's interests (to go outside naked) with their interests (to have their child

---

[50] Sunstein, *Fifty Shades of Manipulation*, *supra* note 12.

[51] *See, e.g.*, Eldar Shafir, *Manipulated as a Way of Life*, 1 J. MKTG. BEHAV. 245, 245 (2016) ("Being manipulated is an integral part of the human condition. It is unavoidable and happening all around us; yet, it has not penetrated our naive view of the autonomy in our decisions."); Shlomo Sher, *A Framework for Assessing Immorally Manipulative Marketing Tactics*, 102 J. BUS. ETHICS 97, 97 (2011) ("[A] marketing tactic is manipulative if it is intended to motivate by undermining what the marketer believes is his/her audience's normal decision-making process either by depiction or by playing on a vulnerability that the marketer believes exists in his/her audience's normal decision-making process."); *see* VANCE PACKARD, THE HIDDEN PERSUADERS 1 (1957); *see also* JOHN KENNETH GALBRAITH, THE AFFLUENT SOCIETY 155–56 (1958) (noting that this is not to say that unseemly persuasion or marketing is tasteful or even morally appropriate at times—only that persuasion is not the phenomenon of interest for this Article).

[52] Allen Wood, *Coercion, Manipulation, Exploitation*, *in* MANIPULATION: THEORY AND PRACTICE 31 (2014). Wood suggests that different tactics could be seen as manipulative—even within the definition of covertly undermining a target's decision-making towards the manipulator's interests—such as lying, misleading, encouraging false assumptions, and fostering self-deception. Here, this Article focuses on the leveraging of vulnerabilities, which could use lying but need not.

go outside with clothes on). Online, firms can leverage a consumer's known vulnerabilities—addiction to gambling, concern for a family member's depression, or a pending divorce—to shift the individual's decision from the individual's current interests towards the firms' interests. This approach, which focuses on the divergence of interests, leaves open the possibility that manipulation could be within interests that align with societal norms, an ethic of care, and respect for human dignity.[53] As Professor Ido Kilovaty summarizes, "[m]anipulation by itself is not an absolute evil. Rather, it depends on whether there is an alignment of interests between the subject and the manipulator, both on the individual and collective levels."[54]

Detailed individualized information in the hands of a firm with interests divergent from consumers is normally considered dangerous. For example, Professor Roger Allan Ford, who studies malicious actors that access consumer data to scam people, suggests that data traffickers aid scammers in using hyper-targeted ads "to reach the most promising victims, hide from law-enforcement authorities," and develop better and more effective scams by providing scammers access to consumers' data.[55] Relatedly, both Kilovaty and Calo analogize to data breach law in recognizing the potential misuse of breached personal information by the actors holding such information because their interests are not aligned with consumers.[56] Thus far, scholarship has focused on scammer and cybersecurity threats as the malicious actors of concern.

But manipulation need not only be carried out by overtly malicious actors that seek to break the law. As noted by Professors Lina Khan and David Pozen, technology companies that control user data have interests divergent from the well-being of their users.[57] In fact, the authors argue (contrary to this Article) that data controllers'

---

[53] Such targeted manipulation is rare and within well-defined relationships. Here, the target's ability to act in their own interest is seen as limited. For example, the parent/child or caregiver/charge relationships often have manipulation when the target cannot care for themselves.

[54] Kilovaty, *supra* note 32, at 466.

[55] Roger Allan Ford, *Data Scams*, 57 HOUS. L. REV. 111, 111 (2019).

[56] *See generally* Kilovaty, *supra* note 32; Calo, *supra* note 8.

[57] Khan & Pozen, *supra* note 42, at 503.

interests are in *perpetual* conflict with their users.[58] According to Khan and Pozen, data brokers, data traffickers, ad networks, and data controllers are all similarly situated with interests that are, at best, not aligned with consumers and are, at worst, perpetually divergent from consumers' interests.[59] This Article need not adopt Khan and Pozen's idea of perpetual conflicts of interest to acknowledge that data traffickers can have interests that diverge from consumers and that few market forces exist to align these interests.[60]

The phenomenon of interest herein focuses on interests diverging between the manipulator and the target and differs from two alternative definitions of manipulation that focus on either (a)

---

[58] "Even if one accepts, for argument's sake, the soundness of the predatory/nonpredatory distinction in this context—although this soundness doubtful—it is unclear how a digital fiduciary is supposed to fulfill its duty of loyalty to users, even under conditions of profound and 'perpetual' conflict." *Id.* at 513. Khan and Pozen's argument shows the danger in using maximizing shareholder wealth as an operating mission statement in running a company. See Lynn Stout and Freeman, Wicks, and Parmar for the standard argument against relying on "shareholder wealth maximization" as necessary, useful, or helpful. *See* R. Edward Freeman et al., *Stakeholder Theory and "The Corporate Objective Revisited*," 15 ORG. SCI. 364, 364 (2004); LYNN A. STOUT, THE SHAREHOLDER VALUE MYTH: HOW PUTTING SHAREHOLDERS FIRST HARMS INVESTORS, CORPORATIONS, AND THE PUBLIC 10–12 (2012).

[59] Empirical studies support the idea that data aggregators and hackers have similarly divergent interests from consumers: Consumers distrust firms that have been hacked and also distrust firms that sell their information to a data aggregator *to the same degree.* Kirsten Martin, *Breaking the Privacy Paradox*, 30 BUS. ETHICS Q. 65, 65 (2020). As Professor Ryan Calo aptly suggests, legal intervention is justified whenever there is a divergence between these interests, leading to one side leveraging this gap in information to her own benefit. Calo, *supra* note 8, at 1023.

[60] As this Author has noted previously, data aggregators and the "Big Data" industry are in a similar position to the banks with credit default swaps in 2008: Neither have any natural market forces to ensure that the interests of the people impacted (users, citizens) are considered. Data aggregators are free to collect any information and will pay top dollar for even the lowest quality information and with the least privacy expectations respected. Similarly, banks in 2008 were free to collect mortgages of low quality and with little to no requirements respected. Both are able to make money while others take on the risks. Kirsten Martin, *Data Aggregators, Consumer Data, and Responsibility Online: Who is Tracking Consumers Online and Should They Stop?*, 32 INFO. SOC'Y 51, 51 (2016).

the "rationality" of the target's decision or (b) the inappropriateness of the target's decision. This first definition of manipulation, a broader approach, focuses on the degree that the target's decision is deemed "rational," wherein manipulators are those that circumvent a target's rational decision-making process.[61] Someone is said to have been manipulated if their decision is judged as not rational *enough*. For example, behavioral economist Cass Sunstein judges a decision as being manipulated "if it does not sufficiently engage or appeal to people's capacity for reflective and deliberate choice."[62]

However, defining manipulation solely as that which undermines "rationality" is problematic. First, only a small group of people[63] actually make decisions in a manner that is consistent with

---

[61] *See* Shaun B. Spencer, *The Problem of Online Manipulation*, 2020 U. ILL. L. REV. 959, 963 (2020); Julia Hanson et al., *Taking Data Out of Context to Hyper-Personalize Ads: Crowdworkers' Privacy Perceptions and Decisions to Disclose Private Information*, CHI 2020 Paper 1, 2 (2020); Kilovaty, *supra* note 32, at 457.

[62] Sunstein, *supra* note 12, at 213. For example, Anne Barnhill includes decision-making that fall short of ideals for "belief, desire, or emotion." She focuses on deliberative versus using heuristics, and that is tied to not acting rationally or to advance their own self-interest. Barnhill, *supra* note 13, at 72. Or, to engage with intuitive thinking or non-verbal. Becher & Feldman, *supra* note 13, at 2. Or, to even just attempt to influence someone's decision-making. RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 6 (2008). *See also* Moti Gorin, *Do Manipulators Always Threaten Rationality?*, 51 AM. PHIL. Q. 51, 51 (2014). And, "human choice is assumed to be made by a mentally competent, fully informed individual, through a process of rational self-deliberation." Michal S. Gal, *Algorithmic Challenges to Autonomous Choice*, 25 MICH. TECH. L. REV. 59, 75–76 (2018) (citing Isaiah Berlin). "Manipulation, broadly conceived, can perhaps be understood as intentionally causing or encouraging people to make the decisions one wants them to make by actively promoting their making the decisions in ways that rational persons would not want to make their decisions." THOMAS E. HILL, JR., AUTONOMY AND SELF-RESPECT 33 (1991); *see also* T. M. Wilkinson, *Nudging and Manipulation*, 61 POL. STUD. 341, 345 (2013).

[63] Autistic respondents, it turns out, might be more "rational" decision makers than non-autistic adults, who tend to behave more "intuitively" in their decision-making. *See* Mark Brosnan et al., *Reasoning on the Autism Spectrum: A Dual Process Theory Account*, 46 J. AUTISM & DEV. DISORDERS 2115, 2121 (2016); *see also* Benedetto De Martino *et al*., *Explaining Enhanced Logical Consistency During Decision Making in Autism*, 28 J. NEUROSCIENCE 10746, 10750 (2008) (finding that autistic individuals were "better able to ignore biasing contextual

what researchers call "rational," thereby leaving the majority of people to continually act in ways deemed "irrational," and thus making the designation do little work in differentiating types of decisions.[64] In other words, under this definition, all decisions can be seen as not fully rational. Therefore, if all decisions are not entirely rational, all decisions are possibly manipulated, making manipulation almost impossible to meaningfully identify.[65] Because non-rational decisions are ubiquitous, equating manipulation with non-rational decisions allows scholars to declare that manipulation is everywhere.[66] However, the phenomenon of interest examined in this Article is the tactic of covertly undermining a target's decision

---

information and isolate the critical information"); *see also* George D. Farmer et al., *People with Autism Spectrum Conditions Make More Consistent Decisions*, 28 PSYCH. SCI. 1067, 1073 (2017) ("People with autism spectrum conditions made . . . more conventionally rational decisions."). Rational decisions also remove adaptations that have proven to be evolutionarily desirable, such as group survival and altruistic fairness. *See* Nicolas Baumard et al., *A Mutualistic Approach to Morality: The Evolution of Fairness by Partner Choice*, 36 BEHAV. & BRAIN SCIS. 59, 81 (2013); *see also* Sule Guney & Ben Newell, *Fairness Overrides Reputation: The Importance of Fairness Considerations in Altruistic Cooperation,* 7 FRONTIERS IN HUM. NEUROSCIENCE 1, 2 (2013) ("[T]he Responders seem to engage in actions that are opposite to their self-interest, in order to maintain the fairness norms between parties. Thus, fairness considerations seem to override the self-regarding/rational motives."); *see also* Ernst Fehr & Simon Gächter, *Fairness and Retaliation: The Economics of Reciprocity*, 14 J. ECON. PERSPS. 159, 161 (2000) ("[P]ositive reciprocity is deeply embedded in many social interactions."). The use of "rational" has mistakenly become shorthand for a desirable decision; however, it is no longer clear that rational decisions are desirable and that irrational decisions are not desirable.

[64] *See* Brosnan, *supra* note 63, at 2121.

[65] One reason "rationality" is put forth as a test to determine if someone is manipulated is to maintain the perspective that a "good" decision is not manipulated and a "bad" decision is manipulated—and "rationality" is a go-to (but mistaken) shorthand for "good" decisions. Scholars do this because society thinks manipulation is morally problematic and therefore morally non-problematic things (like using rational decision-making) should not be included. "[I]t may be assumed that forms of interpersonal influence that are generally taken to be morally benign or even exemplary—for example, rational persuasion—cannot be used manipulatively." Gorin, *supra* note 62, at 51.

[66] *See* Shafir, *supra* note 51, at 255.

towards the interests of the manipulator.[67] Thus, this Article does not focus on whether the target's decision-making is deemed rational or not.[68]

Alternatively, a narrower definition of manipulation requires that the end-goal of the manipulator be undesirable. For example, Professor Tal Zarsky uses the standard of what is socially unacceptable, where manipulation is "a process in which firms strive to motivate and influence individuals to take specific steps and make particular decisions in a manner considered to be socially unacceptable."[69] Similarly, Professor Robert Noggle offers a frequently-used definition of manipulation that rests on the intention of the manipulator to move a target's decision in such a way that even the manipulator would not approve of the decision; scholars Christian Coons and Michael Weber describe Noggle's viewpoint as follows: "[M]anipulation is influence that attempts to get the target to stray from [the influencer's] ideals or rational standards for belief, desire, and emotion."[70] Noggle's version of manipulation "involves influencing in ways the influencers could not themselves

---

[67] However, making rationality the standard for non-manipulation is also used to judge the tactic of nudges, dark patterns, adaptive choice architectures, and invisible influence in general. *See* Becher & Feldman, *supra* note 13, at 459; *see also* Wilkinson, *supra* note 62, at 341 (explaining nudges as a subtle method of influencing human behavior); Thaler & Sunstein, *supra* note 62, at 1; Daniel Susser, *Invisible Influence: Artificial Intelligence and the Ethics of Adaptive Choice Architectures*, PROC. 2019 AAAI/ACM CONF. AI, ETHICS & SOC. 1, 1 (2019). *See also* Arnuesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 PROC. ACM HUM.-COMPUT. INTERACTIONS 81:1, 1 (2019) (examining dark patterns and recommending policies to mitigate potential harm to consumers).

[68] Professor Ryan Calo takes a similar approach in his seminal work where he focuses on the ability of firms to exploit consumers' general tendency to act irrationally. Calo, *supra* note 8, at 1032–33.

[69] Zarsky, *supra* note 46, at 158. For Professor Zarsky, manipulation is based on a standard of rational decision-making, which is desirable: "Entities collecting vast personal information about individuals will use insights they have learned to influence individuals in ways we consider to be unfair and thus unacceptable, and therefore must be stopped." *Id.* at 168–69.

[70] Christian Coons & Michael Weber, *Manipulation: Investigating the Core Concept and Its Moral Status*, MANIPULATION: THEORY & PRAC. 1, 11 (2014); *see also* Robert Noggle, *Manipulative Actions: A Conceptual and Moral Analysis*, 33 AM. PHIL. Q. 43, 45 (1996) (outlining the various types of manipulation).

accept."[71] Moreover, according to Noggle, an act is not manipulative if the manipulator (or influencer) "is sincere, that is, in accordance with what the influencer takes to be true, relevant, and appropriate."[72]

This approach creates a standard of manipulation that is almost never met; according to this paternalistic view of manipulation, manipulators frequently believe their end-goal or interests are aligned with their target. And, sometimes manipulators with this perspective do act in the best interest of the target, such as when parents manipulate their children to put on clothes in the winter or when caregivers manipulate a disabled patient to take their medicine or take a shower. Here, these manipulators are in a position of caregiving with the expectation that their interests will trump the preferences of their charge—a charge who is deemed to need help and unable to make decisions for themselves. More importantly, relying on manipulators themselves to admit that their interests for a target are inappropriate leaves a glaring hole for manipulators to claim they are acting in the best interests of their targets. In fact, marketers likewise frequently defend their tactics as being in the best interest of consumers.[73]

---

[71] Coons & Weber, *supra* note 70, at 14.

[72] Noggle, *supra* note 70, at 50.

[73] For example, an industry trade group, called the Network Advertising Initiative, contends that targeted advertising provides consumer services and content for free, thereby helping the economy. *Understanding Digital Advertising*, NAI, https://www.networkadvertising.org/understanding-online-advertising/ [https://perma.cc/DR77-XKHA] (last visited Dec. 20, 2021). In reaction to a *Wall Street Journal* article on how targeted advertising benefits ad networks and data traffickers but not consumers or publishers doing the advertising, a chief marketing office ("CMO") claimed that, "[a]s most consumers know, advertising relevant to their interests gives them a better experience online. For marketers it's an efficient way to reach their customers." David Doty, *A Reality Check on Advertising Relevancy and Personalization*, FORBES (Aug. 13, 2019, 12:51 PM), https://www.forbes.com/sites/daviddoty/2019/08/13/a-reality-check-on-advertising-relevancy-and-personalization/#7765e9397690 [https://perma.cc/T4TF-7MGK]. The CMO was reacting to a study analyzing who benefits from hyper-targeted advertising that stated, "when advertisers can highly personalize ads, they are . . . reaching narrower consumers' segments where the competition may be drastically reduced . . . potentially leading to a reduction in

Manipulation's "wrongness" is not necessarily because the end goal is bad, irrational, or socially undesirable, but is instead because manipulation undermines the targets as the authors of their own decisions, and attempts to steer those decisions towards the manipulator's interests.[74] Manipulation here is agnostic to the decision-making process or interests of the target. The target may or may not be self-interested, a slow deliberator, immune to sensory signals, or online. Regardless, the manipulator wants to hijack the target's decision towards the manipulator's own preferences and goals—which diverge from the target's—in a way that covertly leverages the target's weaknesses or vulnerabilities. It is the divergence of these interests that makes targeted manipulation particularly important for law and economics.

C. Manipulation in Economics

Targeted manipulation, as in, the leveraging of individualized knowledge to exploit a target's vulnerabilities to covertly undermine their decision-making, has been identified as theoretically possible, but unlikely, by two overlapping fields in economics: (1) advertising and (2) price discrimination.

First, the economics of advertising examines the costs and benefits of advertising and marketing tactics.[75] A subset of scholarship has focused on the economics of information in product promotion, as with hyper-targeted advertising, to include the use of psychographic profiling.[76] Hyper-targeted advertising is framed as efficient so that "advertising is only shown and designed for a select

---

the publisher's revenue." Veronica Marotta, et al., *Online Tracking and Publishers' Revenues: An Empirical Analysis* (May 2019) (preliminary draft).

[74] Susser, Roessler & Nissenbaum, *supra* note 15, at 17; *see also* Wood, *supra* note 52, at 17–18 ("[W]hen getting others to do what you want is morally problematic, this is not so much because you are making them worse off (less happy, less satisfied) but, instead, it is nearly always because you are messing with their *freedom*—whether by taking it away, limiting it, usurping it, or subverting it.").

[75] *See generally* THE ECONOMICS OF ADVERTISING (Kyle Bagwell ed., 2001) (presenting influential scholarship on the economics of advertising).

[76] *See* Burkell & Regan, *supra* note 29, at 1.

group of consumers who stand to gain most from this information."[77] As noted by Professor Catherine Tucker, "at first glance[,] the fact that new digital technologies are enabling more informative advertising would appear to indirectly increase a consumer's potential utility."[78] Better information in the hands of marketers is assumed to benefit advertisers by increasing efficiency and to benefit consumers by showing only relevant ads.[79] A key assumption in the economics of advertising is that data collectors or data traffickers—those who gather and use the consumer data for advertising—are actors with interests aligned with the target, and this apparent alignment is why these scholars may assume that the use of information is a benefit to consumers.

However, the economics of advertising, including product placement and promotion, struggles with incorporating the preferences of the consumer in the analysis when it comes to privacy

---

[77] Catherine E. Tucker, *The Economics of Advertising and Privacy*, 30 INT'L J. INDUS. ORG. 326, 326 (2012) ("[A]n advertiser might track whether someone visits a website that deals with new babies' health issues and then use that information to serve them ads. Alternatively, an advertiser could use information that a person has posted about themselves on a social networking website such as Facebook to identify new mothers."); *see also* Avi Goldfarb & Catherine Tucker, *Digital Economics*, 57 J. ECON. LITERATURE 3, 3 (2019); David S. Evans, *The Online Advertising Industry: Economics, Evolution, and Privacy*, 23 J. ECON. PERSPS. 37, 56 (2009) ("These detailed data on browsing enable providers of online advertising to provide higher-quality prospects to advertisers and to therefore charge more for the advertising inventory they supply.").

[78] Tucker, *supra* note 77, at 326.

[79] Goldfarb and Tucker show that the evidence is mixed in terms of targeted advertising. While Goldfarb and Tucker's 2011 article (Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, 57 MGMT. SCI. 57 (2011)) is frequently cited to establish that privacy regulations could limit the ability of firms to tailor advertising to a consumer's behavior and may reduce online advertising effectiveness, their more recent work is less cited, which found that dynamic retargeted ads are, on average, less effective than their generic equivalent. Avi Goldfarb & Catherine Tucker, *Online Display Advertising: Targeting and Obtrusiveness*, 30 MKTG. SCI. 389, 389 (2011); *see also* Tal Z. Zarsky*, Online Privacy, Tailoring, and Persuasion*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY 209, 209–24 (2006); Avi Goldfarb & Catherine Tucker, *Why Managing Consumer Privacy Can Be an Opportunity*, MITSLOAN (Mar. 19, 2013) https://sloanreview.mit.edu/article/why-managing-consumer-privacy-can-be-an-opportunity/ [https://perma.cc/3GDQ-NLZ2].

expectations, trust, and overall unease with advertising and the required data-tracking.[80] Professor Catherine Tucker has specifically identified the issue of the intrusiveness of data collection as: "[C]onsumers may be wary of being tracked too closely by firms and then firms using this information to tailor prices"—a concern also identified by Professors Alessandro Acquisti and Hal Varian.[81] Scholars studying the economics of information and advertising have identified this problematic tracking tactic—wherein firms gain access to intimate consumer information and use that information to covertly influence consumer decisions—but have yet to sufficiently engage with what the prevalence of manipulation means for the current advertising industry.

Second, the economics of price discrimination analyzes when firms differentiate prices across various populations of customers. Pricing can be based on coupons, group identification, volume of

[80] "There is no clear economic literature that helps factor such [consumer] distaste into the standard utility model." Tucker, *supra* note 77, at 327; Evans, *supra* note 77, at 56; *see* Qiaowei Shen & J. Miguel Villas-Boas, *Behavior-Based Advertising*, 64 MGMT. SCI. 2047, 2047 (2018); *see also* Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LITERATURE 442, 442 (2016). As noted by Goldfarb and Tucker, "[i]n general the economics literature on privacy, both offline and online, grapples with the question of how privacy should be treated in terms of the consumers' utility function." Goldfarb & Tucker, *supra* note 77, at 22. Consumers may resist having advertising platforms collect detailed information about their browsing behavior. *See* Evans, *supra* note 77, at 52. Seen as a cost, consumer annoyance results from sending advertising messages to consumers based on their past purchase behavior. *See* Shen & Villas-Boas, *supra* note 80, at 2047. Acquisti, Taylor, and Wagman note that "national surveys have consistently found widespread evidence of significant privacy concerns among internet users. From the standpoint of self-interested individual behavior, the economic motive behind concerns for privacy is far from irrational. It is nearly self-evident. If it is true that information is power, then control over personal information can affect the balance of economic power among parties." Acquisti, Taylor & Wagman, *supra* note 80, at 445.

[81] Tucker, *supra* note 77, at 326. This concern was also identified in a similar article by Professors Alessandro Acquisti and Hal Varian. *See* Alessandro Acquisti & Hal R. Varian, *Conditioning Prices on Purchase History*, 24 MKTG. SCI. 367, 367 (2005).

product, and other methods.[82] Personalized pricing (also referred to as first-degree price discrimination, customized pricing, or targeted pricing), represents a pricing strategy "whereby firms charge different prices to different consumers based on their willingness to pay."[83] As noted in a symposium on the economics of price discrimination, "[W]e are approaching a world in which each consumer will be charged a personalized price for a personalized product or service."[84] For example, Professors Peter Seele, Claus Dierksmeier, Reto Hofstetter, and Mario Schultz have advanced a classic example of the choice to sell Coca-Cola, not based on a location or even the location's temperature, but based on a consumer's willingness to pay.[85] Given the evolution of online marketing, a concern is that firms might offer, for example, Coca-Cola based on whether someone is diabetic, addicted to sugar, or, perhaps, at a low emotional point. Building on consumer data, pricing algorithms can estimate consumers' willingness to pay, or,

---

[82] Curtis R. Taylor, *Consumer Privacy and the Market for Customer Information*, RAND J. ECON., 631, 640 (2004); Gerhard Wagner & Horst Eidenmüller, *Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions*, 86 U. CHI. L. REV. 581, 581 (2019). Third-degree price discrimination consists of offering different pricing for different groups of people based on observable characteristics—perhaps coupons of versioning. Goldfarb & Tucker, *supra* note 77. Second-degree price discrimination is the offering of different pricing and allowing consumers to choose the pricing that suits them (volume pricing). *Id.* First degree price discrimination includes personalized pricing. *Id.* In addition, pricing in general can include what product is offered and at what price to each consumer or group of consumers. *Id.*

[83] *See* Vidyanand Choudhary et al., *Personalized Pricing and Quality Differentiation*, 51 MGMT. SCI. 1120, 1120 (2005); *see also* Paul Heidhues & Botond Kőszegi, *Naïveté-Based Discrimination*, 132 Q. J. ECON. 1019, 1019 (2017); Acquisti & Varian, *supra* note 81, at 367; Hal Varian, *Artificial Intelligence, Economics, and Industrial Organization* (Nat'l Bureau of Econ. Rsch., Working Paper No. 24839 2018).

[84] Oren Bar-Gill, *Algorithmic Price Discrimination When Demand Is a Function of Both Preferences and (Mis)perceptions*, 86 U. CHI. L. REV. 217, 217 (2019). It should be noted that not all find personalized pricing to be realistic—perhaps because the current incarnation of personalized pricing is so problematic, as examined here. *See* Varian, *supra* note 83.

[85] Peter Seele et al., *Mapping the Ethicality of Algorithmic Pricing: A Review of Dynamic and Personalized Pricing*, 170 J. BUS. ETHICS 697, 697 (2019).

as Professors Zubin Xu and Anthony Dukes state, algorithms can gain "superior knowledge" by understanding consumer preferences better than the consumers themselves.[86]

In one of the first examinations of personalized pricing, Acquisti and Varian analyzed conditioning prices on consumers' purchase history.[87] At the time, the personalized pricing analysis assumed consumers (1) knew the firms conducting the price discrimination and (2) were emboldened to take their business elsewhere if the price discrimination was unwanted.[88] Further, it was assumed that the price discrimination would make the pricing more accurate and efficient and, therefore, beneficial to consumers (or they would otherwise leave the transaction).[89]

However, these assumptions no longer hold given the current capabilities in online marketing. First, firms seeking to price discriminate are unknown to consumers, rendering consumers unable to take any market action to stop the collection of information necessary to engage in the problematic price discrimination (or targeted manipulation in this Article's parlance). For example, in their analysis of price discrimination, authors Professors Peter Seele, Claus Dierksmeier, Reto Hofstetter, and Mario Schultz note that "[w]hat remains invisible for the eye of most consumers, is the fact that their online behavior creates a long data trace consisting of

[86] Zibin Xu & Anthony Dukes, *Product Line Design Under Preference Uncertainty Using Aggregate Consumer Data*, 38 MKTG. SCI. 669, 669 (2019).

[87] Acquisti & Varian, *supra* note 81, at 367.

[88] *Id.* ("Although sellers can now easily use price-conditioning strategies, consumers are far from defenseless. No one is forced to join a loyalty program. It is relatively easy to set one's browser to reject cookies or to erase them after a session is over. Consumers can use a variety of credit cards or more exotic anonymous payment technologies to make purchases anonymous or difficult to trace. In addition, consumers can voice their displeasure for pricing policies perceived as discriminatory or intrusive . . . .").

[89] For example, assume that "even though sellers can post prices, observe choices, and condition subsequent price offers on observed behavior, buyers are also able to hide the fact that they bought previously. Hence, it is likely that sellers will have to offer buyers some benefits to induce them to reveal their identities." *Id.* at 368.

personal characteristics, such as location data, browsing and purchasing history, social media posts and 'likes,' and so on."[90]

Second, consumers cannot be considered emboldened.[91] As noted more recently by Professors Alessandro Acquisti, Curtis Taylor, and Liad Wagman:

> Personal data is continuously bought, sold, and traded among firms (from credit-reporting agencies to advertising companies to so-called 'infomediaries,' which buy, sell, and trade personal data), but consumers . . . do not have access to those markets: they cannot yet efficiently buy back their data, or offer their data for sale.[92]

Finally, current online digital marketing and pricing techniques are not necessarily more accurate or efficient for the consumer. Recent scholarship on the economics of personalized pricing has raised concerns over manufacturing preferences and artificially shifting consumption patterns.[93] "When price discrimination targets misperceptions, specifically demand-inflating misperceptions," price discrimination may hurt consumers and may reduce efficiency.[94] The economics of price discrimination has (until recently) been able to hold constant consumer preferences or has assumed that hyper-targeting and personalized pricing is beneficial, therefore making the type of targeted consumer manipulation, that is the subject of this Article, not a concern.[95]

---

[90] Seele et al., *supra* note 85, at 705.

[91] Aquisti, Taylor & Wagman, *supra* note 80, at 447; *see* David Streitfeld, *On the Web, Price Tags Blur*, WASH. POST (Sept. 27, 2000) https://www.washingtonpost.com/archive/politics/2000/09/27/on-the-web-price-tags-blur/14daea51-3a64-488f-8e6b-c1a3654773da/ [https://perma.cc/8WAM-T2FX].

[92] Acquisti, Taylor & Wagman, *supra* note 80, at 447.

[93] "When the seller 'manufactured' the preferences of the buyer, it is no longer clear that a contract of sale, entered into voluntarily, maximizes the welfare of both parties. The function of the bargained-for contract, to ensure optimal satisfaction of preferences for both sides, becomes moot. And with it, the concept of social welfare, understood as the aggregate of individual well-being, becomes illusory." Wagner & Eidenmuller, *supra* note 82, at 602.

[94] In this situation, for economists, the "actual" demand curve is supplemented by the perceived demand curve—where consumers are manipulated into believing they have a demand. Bar-Gill, *supra* note 84, at 217.

[95] Justin P. Johnson notes that the cost of losing the trust of consumers is not included at all in the calculation to use manipulative tactics in marketing, such as

In sum, both the economics of advertising and the economics of price discrimination have identified the often assumed-away scenario of using intimate knowledge to covertly manipulate a consumer through advertising, product placement, or pricing. Professors Gerhard Wagner and Horst Eidenmuller nicely summarized this conclusion in a recent analysis of the economics of personalized pricing: "In traditional markets, sellers do not know the 'weak spots' of an individual customer and thus are unable to turn them into 'sweet spots' for themselves."[96] The possibility of a firm gaining a position of power to manipulate consumers—with intimate knowledge of consumers, as well as the reach to covertly target their decision-making—has always been a possibility in economics but was considered highly unlikely with empowered and knowledgeable consumers.[97] More recent work in economics has begun to grapple with the reality consumers face—where firms are now in the position to manipulate millions online without any governance or safeguards in place.[98]

III. MANIPULATION AND CONSUMER CHOICE

Online firms are now in the position to manipulate consumers with data about individuals' weaknesses to covertly influence the decisions of targets. This scenario was predicted as possible, even worrisome, by economists but unlikely due to presumed structural

psychometric profiling and hyper-targeted advertising. Justin P. Johnson, *Targeted Advertising and Advertising Avoidance*, 44 RAND J. ECON. 128, 128 (2013). Florian Hoffmann, Roman Inderst, and Marco Ottaviani provide a helpful example of never taking into consideration the desires of the object of information: "We derive positive and normative implications depending on the extent of competition among senders, whether receivers are wary of senders collecting personalized data, and whether firms are able to personalize prices." Florian Hoffmann, Roman Inderst & Marco Ottaviani, *Persuasion Through Selective Disclosure: Implications for Marketing, Campaigning, and Privacy Regulation*, 66 MGMT. SCI. 4958, 4958 (2020).

[96] Wagner & Eidenmuller, *supra* note 82, at 607.

[97] Stigler, *supra* note 1, at 213.

[98] The next Part covers this idea. *See, e.g.*, Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age*, 30 J. CONSUMER PSYCH. 736 (2020).

and market barriers.[99] Economists previously assumed that intimate information would remain only in the hands of those whose interests aligned with the individual and where consumers would know the firm that used their information for promotion, placement, or pricing.[100] In other words, the underlying assumption was that consumers would always be enabled to prevent their information from falling into the hands of firms capable of manipulating them.[101] This assumption is normally very reasonable; offline market actors do not disclose information about preferences, concerns, forecasts, or other data without safeguards in place to protect against possible manipulation.[102]

Importantly, firms are in the position to manipulate consumers, thereby undermining an individual consumer's ability to enact their preferences through choice. A defining feature of this tactic is to steer the target's decision away from their interests and towards the manipulator's interests; currently, data-trafficking firms are in a position to manipulate consumers across markets—when shopping online, when looking for a doctor, when researching universities, when pricing a loan, etc.

Next, this Article examines the danger of targeted manipulation in undermining consumer choice in the market. Society generally seeks to preserve consumer choice, where choice is meaningful and indicative of consent to a transaction. Choice-as-consent is important across markets, not only to preserve the individual as the author of their own decision,[103] but also to ensure the preferences of the individual are enacted in their decisions, and that those transactions and the market are efficient and legitimate.[104] In fact, as this Article explores in more detail below, authentic consent is critical to markets and economics. This Article positions targeted online manipulation—the covert leveraging of vulnerabilities to

---

[99] *See supra* Part II.C.; *infra* Part IV.A.

[100] *See supra* Part II.C.

[101] *See supra* Part II.C.

[102] *See infra* Part III.C.

[103] *See* Susser, Roessler & Nissenbaum, *supra* note 15, at 17.

[104] *See* Friedrich August Hayek, *The Use of Knowledge in Society*, 35 AM. ECON. REV. 519, 519 (1945); R. H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 42–44 (1960); Zarsky, *supra* note 46, at 168.

undermine a target's decision-making—as a close cousin to fraud and coercion in undermining consumer choice.

A. Choice-as-Consent

Before agreements and contracts and before transaction costs and safeguards, lies an assumption that individual choice is meaningful and exemplifies the operationalization of a market actor's preferences. A choice to agree or transact in the market is unburdened by coercion, fraud, and government intervention. Words like "free" and "voluntary private bargaining" are frequently used to explain market actors and transactions.[105] In deciding to transact, individuals search and gather information as to the terms, bargain over those terms, and then make a decision based on their knowledge of their preferences, needs, and information.[106] That choice is the consumer's enactment of preferences, or as close as one can get to such an enactment. The principle is that one protects the voluntary character of an exchange and seeks to identify actions that could undermine choice-as-consent.[107]

Choice-as-consent is the air that the modern economist breathes: "[B]y choosing, individuals reveal that they agree with or consent to

---

[105] As noted by Milton Friedman, economic exchanges are market exchanges if "individuals are effectively free to enter or not to enter into any particular exchange, so that every transaction is strictly voluntary." MILTON FRIEDMAN, CAPITALISM AND FREEDOM 14 (1962). Hayek, *supra* note 104, at 524 ("If we can agree that the economic problem of society is mainly one of rapid adaptation to changes in the particular circumstances of time and place, it would seem to follow that the ultimate decisions must be left to the people who are familiar with these circumstances, who know directly of the relevant changes and of the resources immediately available to meet them."); *see also* Gordon R. Foxall, *The Behavior Analysis of Consumer Choice: An Introduction to the Special Issue*, J. ECON. PSYCH. 581–82 (2003). Coase defends choice as better than any interference. Coase, *supra* note 104, at 1. Arrow starts his argument with a "chooser" for social choice and likens voting to market choice. Kenneth J. Arrow, *A Difficulty in the Concept of Social Welfare*, 58 J. POL. ECON. 328, 331 (1950).

[106] *See* Coase, *supra* note 104, at 114; *see generally* R. H. COASE, THE FIRM, THE MARKET, AND THE LAW (1988).

[107] *See* 3 JAMES M. BUCHANAN & GORDON TULLOCK, THE CALCULUS OF CONSENT: LOGICAL FOUNDATIONS OF CONSTITUTIONAL DEMOCRACY 49 (Ann Arbor: Univ. Mich. Press, 1962).

the conditions under which the choice is made."[108] The argument behind the exaltations of choice-as-consent is that each individual is best able to identify, weigh, argue, and act in their best interest. For example, when choosing a mortgage lender, the individual determines which factors (e.g., timelines, rate, responsiveness, etc.) are important to them—their choice reflects their preferences. Choice-as-consent critically allows individuals to retain autonomy and choose since "individuals know better than anyone else what is best for them."[109]

In undermining an individual's choice in the market, manipulation closely mirrors coercion and fraud. Philosopher Joseph Raz links manipulation to coercion where both tactics "subject the will of one person to that of another," which violates their "independence and is inconsistent with [their] autonomy."[110] Where coercion subverts the choice of the target by physically taking away options, manipulation subverts the choice of the target by perverting how individuals make decisions and form preferences.[111] Where the target must be aware of coercion for it to work, manipulation only works if hidden from the target. The manipulator, by distorting the reality of the target's situation, must have the individual believe that they made their own decision.[112] Table 1 below summarizes how manipulation, fraud, coercion, and persuasion work to undermine consumer choice and highlights how

---

[108] Alain Marciano, *Freedom, Choice and Consent. A Note on a Libertarian Paternalist Dilemma*, 32 HOMO OECONOMICUS 287, 288 (2015).

[109] Gal, *supra* note 62, at 76. In doing so, individuals are able to choose based on their preferences, as formed within their lived experience. *Id.*

[110] RAZ, *supra* note 15, at 378. Raz states that autonomy is part of a social ideal and is opposed to a life of coerced choices. *Id.*

[111] *Id.* at 377–78. As noted by Wilkinson, "manipulation involves the perversion of a decision-making process. Whereas coercion uses threats, which involve changing the costs of selecting certain options, manipulation involves some underhand interference with the ways in which people see their options." Wilkinson, *supra* note 62, at 345. For Raz, manipulation "perverts the way [a] person reaches decisions, forms preferences or adopts goals." RAZ, *supra* note 15, at 377–78.

[112] Konstantinos Kalliris, *Self-Authorship, Well-Being and Paternalism*, 8 JURIS. 23, 30 (2017).

targeted manipulation aligns more closely with coercion and fraud than with persuasion as a tactic to "influence" decision-making.

Table 1. Comparing Tactics that Undermine Consumer Choice

Factors of Manipulation	**Consumer Choice Targeting Tactics**			
	Manipulation	**Coercion**	**Fraud**	**Persuasion**
Goal to Subvert Target's Interests	Y	Y	Y	N
Hidden	Y	N	Y	N
Undermine Decision-making	Y	Y	Y	N
Exploit Vulnerability	Y	Y	N	N

* Y = yes; N = no

Professor Eric Posner perhaps best links manipulation to choice: Manipulation "causes a person to act against his own interest, and for the interest of someone else, in a setting where the victim cannot easily protect himself by relying on common sense or ordinary willpower."[113] Alternatively, Professor Martin Wilkinson posits that manipulation "is intentionally and successfully influencing someone using methods that pervert choice."[114]

B. Why Society Protects Choice

Manipulation is in a family of tactics that undermines consumer choice in the market—tactics which are the subject of regulations and safeguards.[115] One protects choice for three reasons: (1) the

[113] Posner, *supra* note 15, at 6.
[114] Wilkinson, *supra* note 62, at 347.
[115] This family of tactics includes fraud, coercion, misrepresentation, undue influence, and others.

autonomy of the individual; (2) the efficiency of individual transactions; and, (3) the legitimacy of the market.

1. Autonomy

As philosopher Raz summarizes, "[t]he ideal of personal autonomy is the vision of people controlling, to some degree, their own destiny, fashioning it through successive decisions throughout their lives."[116] Autonomy is critical for individuals to "have unique access to their situations, their constraints, and their tastes."[117] This drive for autonomy is the same drive for liberty and provides the grounding for our political, social, and economic lives.[118] As noted by philosopher Isaiah Berlin:

> [T]he word 'liberty' derives from the wish on the part of the individual to be his own master. I wish my life and decisions to depend on myself, not on external forces of whatever kind. I wish to be the instrument of my own, not of other men's, acts of will. I wish to be a subject, not an object to be moved by reasons, by conscious purposes, which are my own, not by causes which affect me, as it were, from outside. I wish to be . . . a doer—deciding, not being decided for . . . .[119]

Autonomy is an end worth protecting, not because maintaining autonomy necessarily optimizes decisions or serves some larger good, but because maintaining autonomy allows an individual to be the author of her own decisions.[120] Someone who is autonomous can evaluate options, assess plans, and decide what is best.[121] As Dr. Konstantinos Kalliris summarizes, "[c]oercion and manipulation undermine autonomy because they interfere with this decision-making process."[122] If individuals are manipulated, "they are deprived of the (full) ability to make choices on their own, simply because they are not given a fair or adequate chance to weigh all variables."[123] Manipulation disrupts a target's capacity for self-

---

[116] RAZ, *supra* note 15, at 369 n.5.

[117] Sunstein, *supra* note 33, at 228.

[118] Burkell & Regan, *supra* note 29, at 1; Amartya Sen, *Liberty and Social Choice*, 80 J. PHIL. 5, 5 (1983); AMARTYA SEN, *Individual Preference as the Basis of Social Choice*, *in* SOCIAL CHOICE RE-EXAMINED 15, 15 (Springer, 1997).

[119] ISAIAH BERLIN, TWO CONCEPTS OF LIBERTY 22 (1958).

[120] Susser, Roessler & Nissenbaum, *supra* note 15.

[121] Kalliris, *supra* note 112, at 8.

[122] *Id.*

[123] Sunstein, *supra* note 12, at 228.

authorship by allowing another to decide how and why the target ought to live.[124] Manipulation's challenge to individual autonomy as self-authorship is "its deeper, more insidious harm."[125]

2. Efficiency

For economists, efficiency is the ultimate rationale for favoring authentic choice and is why economic theory relies on choice.[126] Not allowing consumers to make their own choices based on their preferences and in pursuit of their own interests is considered inefficient and leads to suboptimal transactions.[127] The individual "is the person most interested in his own well-being" and the "ordinary man or woman has means of knowledge immeasurably surpassing those that can be possessed by anyone else."[128] Essentially, the

---

[124] Susser, Roessler & Nissenbaum, *supra* note 29, at 8 ("Making one's own life means freely facing both existential choices, like whom to spend one's life with or whether to have children, and pedestrian, everyday ones. And facing them freely means having the opportunity to think about and deliberate over one's options, considering them against the backdrop of one's beliefs, desires, and commitments, and ultimately deciding for reasons one recognises and endorses as one's own, absent unwelcome influence."). Manipulation "subverts and insults a person's autonomous decision-making." Wilkinson, *supra* note 62, at 345.

[125] Susser, Roessler & Nissenbaum, *supra* note 29, at 1; *see also* Kalliris, *supra* note 112, at 1.

[126] Authentic choice is free from manipulation, coercion, fraud, deception, etc., or as close as one can get.

[127] Zarsky, *supra* note 46, at 172; Calo, *supra* note 8, at 1025. "According to this economically-driven line of thought, a successful manipulation will generate a suboptimal transaction, in which individuals fail to properly exercise their preferences." Zarsky, *supra* note 46, at 172. "[C]onsumers confronted with manipulation eventually do not act in accordance with their preferences, thus leading to suboptimal outcome." *Id.* at 173.

[128] *See* JOHN STUART MILL, ON LIBERTY 70 (1859). According to Mill, "[T]he only purpose for which power can be rightfully exercised over any member of a civilised community, against his will, is to prevent harm to others. His own good, either physical or moral, is not a sufficient warrant. He cannot rightfully be compelled to do or forbear because it will be better for him to do so, because it will make him happier, because, in the opinion of others, to do so would be wise, or even right." *Id.* at 17. Mill is often cited to explain why society supports choice-as-consent at the level of the individual. *See also* Giovanni De Gregorio & Sofia Ranchordas, *Breaking Down Information Silos with Big Data: A Legal Analysis of Data Sharing*, LEGAL CHALLENGES OF BIG DATA (Edward Elgar Publishing, 2020).

individual knows his own tastes, values, interests, and preferences. As Professor Friedrich August Hayek famously argued:

> It is with respect to this [knowledge of the particular circumstances of time and place] that practically every individual has some advantage over all others because he possesses unique information of which beneficial use might be made, but of which use can be made only if the decisions depending on it are left to him or are made with his active cooperation.[129]

Individuals themselves are in the best position to understand their competing demands and preferences and to make the best decision in their interest.[130]

3. Legitimacy

The legitimacy argument for authentic choice can be seen as the culmination of millions of efficient, autonomous decisions. Supporting authentic choice at the level of the individual transaction ensures the greatest autonomy possible in any given situation and allows the individual to decide based on their own values, interests, and preferences. In accordance with this sentiment, Professor Fabienne Peter noted that "[t]he emphasis in economic theory on freedom of choice in the market sphere suggests that legitimization in the market sphere is 'automatic' and that markets can thus avoid the typical legitimization problem of the state."[131] Freedom of choice, for Peter, is the foundation of efficient and autonomous decisions, which allows one to declare the market as legitimate.[132]

Manipulation, in undermining consumer choice, leads to the transactional sins of diminishing the autonomy of the decision

---

[129] Hayek, *supra* note 104, at 521–22.

[130] Jacob Viner, in referencing 18th century philosopher Jeremy Bentham to explain the role of choice, noted that "Bentham, in his general exposition, held that to interfere with a free con- tract in a free market in the supposed interest of the parties, where there was no recognized adverse impact on particular non-participants in the contract, would be to make the absurd assumptions that a government or an official can know better than a man knows what that man wants, and can know better than that man knows what are the most efficient means for him of satisfying his wants." Jacob Viner, *The Intellectual History of Laissez Faire*, 3 J.L. & ECON. 45, 65 (1960).

[131] Fabienne Peter, *Choice, Consent, and the Legitimacy of Market Transactions*, 20 ECON. & PHIL. 1, 1 (2004).

[132] *See id.*

maker and inefficiently allocating resources. These transactional sins aggregate to reduce the legitimacy of the market. In other words, choice-as-consent helps justify the moral legitimacy of transactions as a whole,[133] and markets are legitimate when each transaction is voluntary and free, as in, without coercion, fraud, deception, or manipulation.[134]

C. How to Protect Authentic Choice in the Market

Manipulation is hardly the only problematic behavior that seeks to undermine authentic choice in the market. To preserve market integrity and legitimacy, choice is protected in the market by seeking to eradicate any interference with private preferences.[135] For example, one protects choice by safeguarding market actors from negotiating under duress, as well as by seeking to prevent contractors from acting in bad faith,[136] opportunistically, or unconscionably.[137] Deception is also aggressively governed in the law,[138] including false suggestions; concealment of the truth;

---

[133] Robin West, *Authority, Autonomy, and Choice: The Role of Consent in the Moral and Political Visions of Franz Kafka and Richard Posner*, 99 HARV. L. REV. 384, 384 (1985).

[134] *See, e.g.*, ROBERT NOZICK, ANARCHY, STATE, AND UTOPIA 149 (vol. 5038 New York, Basic Books 1974) (noting that when the Securities and Exchange Commission ("SEC") investigates and prosecutes insider trading and fraud, the SEC does so in pursuit of maintaining legitimacy of the market).

[135] Cass R. Sunstein, *Legal Interference with Private Preferences*, 53 U. CHI. L. REV. 1129, 1129 (1986).

[136] In every contract are the implied duties of good faith and fair dealing in the performance and enforcement of the contract. RESTATEMENT (SECOND) OF CONTRACTS § 205 (A.L.I. 1981); U.C.C. § 1-304 (A.L.I. & UNIF. L. COMM'N 2017). The implied duty of good faith helps to protect consumers by ensuring that parties with whom the consumer contracts act honestly and do not take advantage of the consumer in the performance of their contract. *Id.* The Uniform Commercial Code defines good faith as "honesty in fact and the observance of reasonable commercial standards of fair dealing." U.C.C. § 1-201 (A.L.I. & UNIF. L. COMM'N 2017).

[137] Posner, *supra* note 15, at 267.

[138] Stuart P. Green, *Lying, Misleading, and Falsely Denying: How Moral Concepts Inform the Law of Perjury, Fraud, and False Statements*, 53 HASTINGS L.J. 157, 157 (2001).

deception about facts, opinions, or law; and even intentional ambiguities.[139]

Vulnerable consumers' authentic choice is also protected to maintain choice-as-consent. Vulnerable consumers are those actors in the market with limited ability to authentically consent to a transaction.[140] Vulnerability is not necessarily a permanent attribute of a relationship or an individual, and consumers can move in and out of contexts that make them vulnerable.[141] Individuals are considered vulnerable, for example, during key stages in their lives,[142] when battling health challenges,[143] or when in temporarily vulnerable positions, such as after a hurricane or other natural disaster.[144]

In sum, tactics that undermine choice-as-consent, such as misrepresentation, power imbalance, coercion, and fraud, are problematic because consumer choice under these conditions is not an authentic or actual operationalization of consumers' preferences. As the next Part examines, choice has been actively protected in markets by laws to preserve individual autonomy, transaction efficiency, and market legitimacy.

---

[139] Larry Alexander & Emily Sherwin, *Deception in Morality and Law*, 22 L. & PHIL. 393, 393 (2003).

[140] Targeting vulnerable consumers is part of the dark side of customer relationship management. Gilles N'Goala, *Opportunism, Transparency, Manipulation, Deception and Exploitation of Customers' Vulnerabilities in CRM*, *in* THE DARK SIDE OF CRM: CUSTOMERS, RELATIONSHIPS AND MANAGEMENT 122 (Bang Nguyen, Lyndon Simkin, Ana Isabel Canhoto eds., 2015).

[141] Wided Batat, *An Adolescent-Centric Approach to Consumer Vulnerability: New Implications for Public Policy*, *in* CONSUMER VULNERABILITY 117 (Kathy Hamilton, Susan Dunnett, Maria Piacentini eds., 2015).

[142] Some examples of key stages in life include: puberty, peer rejection, low socioeconomic status, and family disharmony. Agnes Nairn, *Children as Vulnerable Consumers*, *in* CONSUMER VULNERABILITY 93 (Kathy Hamilton, Susan Dunnett, Maria Piacentini eds., 2015).

[143] Health challenges (e.g., examine late-stage AIDS, breast cancer patients, chronic illness, parents of significant disability) impact the agency and identity of the consumer. Marlys J. Mason & Teresa Pavia, *Health Shocks, Identity and Consumer Vulnerability*, *in* CONSUMER VULNERABILITY 159 (Kathy Hamilton, Susan Dunnett, Maria Piacentini eds., 2015).

[144] Ronald Paul Hill & Eesha Sharma, *Consumer Vulnerability*, 30 J. CONSUMER PSYCH. 551, 551, 560 (2020).

D. How Manipulation is Typically Regulated

Typically, the power to manipulate is regulated offline and derives from a specific relationship where one party gains knowledge or power to manipulate a vulnerable target, such as with a lawyer, teacher, doctor, or therapist. In those relationships, rules of professional conduct, laws, and contracts ensure those interests remain aligned even when one party with knowledge and power is in a position to manipulate.

Typically, sharing information with a particular market actor (a firm or an individual) requires trust and other safeguards, such as professional duties, contracts, negotiated alliances, nondisclosure agreements, etc.[145] A supplier might craft a contract, a non-disclosure agreement, or even enter an alliance in order for the supplier to safely share concerns, preferences, forecasts, and risks.

For individuals, such information is also shared in trusted, fiduciary relationships, such as with lawyers, therapists, or advisors. In contrast, individuals do not typically share information freely with marketers or salespersons; for example, an individual generally would not share, with a car salesperson, how poorly their current car is running or changes in their household finances, because the car salesperson could then use that information against the individual's interest.[146] Thus, manipulation is often prevented offline by ensuring market actors with intimate information about a target's vulnerabilities are prevented from using that information against the target.[147]

---

[145] Oliver E. Williamson, *The Theory of the Firm as Governance Structure: from Choice to Contract*, 16 J. ECON. PERSPS. 171, 176 (2002).

[146] Joseph Farrell, *Information and the Coase Theorem*, 1 J. ECON. PERSPS. 113, 117 (1987) ("People with private information may not readily reveal it, especially if they know that it will be used in a decision that affects them.").

[147] Professor Ryan Calo refers to this economic intimacy in a larger argument: Discriminately sharing information between market actors is good for markets. Ryan Calo, *Privacy and Markets: A Love Story*, 91 NOTRE DAME L. REV. 649, 650 (2016). In business, one focuses on a Coasian analysis of the safeguards required to share information—with sharing information considered to be both risky and rewarding for markets and market actors. Jeffrey S. Harrison, Douglas A. Bosse & Robert A. Phillips, *Managing for Stakeholders, Stakeholder Utility Functions, and Competitive Advantage*, 31 STRATEGIC MGMT. J. 58, 58 (2010); Kirsten Martin & Robert Phillips, *Stakeholder Friction*, J. BUS. ETHICS 1, 1 (2021).

IV. ORIGINAL MARKET SIN: PRIVACY-AS-CONCEALMENT

The situation explained above is odd: Firms can collect and covertly use individualized information to undermine consumer decisions. The incarnation of targeted manipulation online divorces the intimate knowledge of the target, as well as the reach used to manipulate, from a specific, trusting relationship. Now, firms—with whom consumers have no relationship—have more information about consumers' preferences, concerns, and vulnerabilities than even their doctors, lawyers, or therapists. In addition, these firms can easily and directly reach specific targets due to the many hyper-targeting mechanisms available online.[148] Yet, consumers are not privy to who has access to their information when a company approaches them with targeted product suggestions or advertising.[149]

Given this economic anomaly, where data traffickers have the intimate knowledge and proximity of a relationship without the governance and trust inherent to such relationships in the market, this Article next examines how firms gain positions of power to exploit vulnerabilities and weaknesses of individuals without the requisite safeguards. Specifically, in a free market, how does information that renders a market actor vulnerable get into the hands of firms whose interests do not align with theirs?

This current market problem—where firms, whose interests do not align with consumers, have the knowledge and position to manipulate consumers—is due to the mistaken notion that disclosed information can be freely shared and used. This perceived free-for-all where, as Professor Helen Nissenbaum notes, "anything goes," relies on privacy as only that which is concealed.[150] By disclosing information, individuals are mistakenly framed as relinquishing any expectation of privacy, and the information is no longer governed by formal or informal norms.[151]

---

[148] *Supra,* Part I.

[149] Plus, firms and individuals are usually on guard to possible manipulation since they know the potential manipulator has information on their vulnerabilities; that is currently not the case online.

[150] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 137 (2004).

[151] Now, individuals in the United States need not even 'disclose' information. In just being, individuals are assumed to be tracked.

After connecting the original sin of the market, using privacy-as-concealment, where disclosed information no longer has privacy expectations, to consumer manipulation, this Article then illustrates the influence of privacy-as-concealment on how privacy is studied and regulated in economics and policy.

A. The Concept of Privacy-as-Concealment

In an important examination of the economics of privacy, Professors Alessandro Acquisti, Leslie John, and George Loewenstein linked privacy-as-concealment to scholarship in the 1970s and 1980s: "The roots of economic research on privacy (which can be found in seminal writings of scholars such as Richard Posner and George Stigler) focus on privacy as the concealment,"[152] where consumer privacy is equated to consumers' ability to conceal information.[153] This definition was useful to the field since privacy-as-concealment is easy to identify and model in economic analyses; market actors would make a binary (and easily measured) decision

[152] Alessandro Acquisti, Leslie K. John & George Loewenstein, *What Is Privacy Worth?*, 42 J. LEGAL STUD. 249, 251 (2013); *see also* Avi Goldfarb, *What Is Different About Online Advertising?*, 44 REV. INDUS. ORG. 115, 251 (2014). Both Posner and Stigler frame the concealment as information that is "private" and the disclosure of information as not private. *See* Richard A. Posner, *The Economics of Privacy*, 71 AM. ECON. REV. 405, 405 (1981); Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 393 (1978); George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 643 (1980).

[153] Stigler and Posner also posit privacy (as concealment) as either increasing or diminishing the "wealth of society," and both make public policy suggestions with privacy-as-concealment as their assumptions and wealth maximization as their goal. Professor Julie Cohen rightly criticizes Posner's goal of "wealth maximization": "Within a liberal market economy, it is an article of faith that both firms and individuals should be able to seek and use information that (they believe) will make them economically better off." Julie E. Cohen, *Privacy, Ideology, and Technology: A Response to Jeffrey Rosen*, 89 GEO. L.J. 2029, 2032 (2000) (reviewing JEFFERY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (2000)). This Article agrees with this second critique of the foundations of the economics of privacy. Here, this Article focuses on the fallacy that privacy is only that which is concealed.

to either conceal information (i.e., protect privacy) or disclose it (i.e., relinquish privacy).[154]

This approach to defining privacy-as-concealment renders privacy inefficient to a functioning market since (in principle) relevant, concealed information could be helpful to better transactions.[155] Thus, privacy-as-concealment fed easily into the economics of information scholarship, which focused on information as being critical for markets to run efficiently, including marriage markets, consumer goods markets, and employment markets.[156] Economists could then summarize: "Privacy is harmful to efficiency because it stops information flows that would otherwise lead to improved levels of economic exchange."[157] Since

---

[154] Contrary to popular musings about privacy having no definitions, privacy definitions fall into three broad categories; concealment is only one. The most popular two are: the "restricted access" version of privacy (that which is private is inaccessible or concealed), and the "control" version of privacy (that which is private is controlled). The standard economic version of privacy is the first definition, whereby information that is concealed is private. This definition is attractive for practical reasons in that it is easy to measure (either someone discloses information or does not) in surveys and in the field. Further, the definition is binary (disclosed or concealed), making models easier. Unfortunately, while privacy-as-concealment is easy to model or make assumptions about, it is not reflective of how people operationalize privacy in their lived experience. Privacy as Contextual Integrity or Privacy as a Social Contract both define privacy as the rules or norms that govern who, what, and how data is gathered and used. Violations of privacy are the breaking of those rules or norms. This concept is further explored below. See Professor Daniel Solove and the anthology edited by Professor Schoemann for overviews of the definition of privacy. *See generally* Ferdinand D. Schoeman, *Philosophical Dimensions of Privacy: An Anthology* (Cambridge Univ. Press, 1984); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PENN. L. REV. 477 (2006) (defining privacy).

[155] Stigler, *supra* note 152, at 625.

[156] Posner, *The Economics of Privacy, supra* note 152, at 405 ("An example is the marriage 'market.' The efficient sorting of females to males in that market is impeded if either spouse conceals material personal information.").

[157] Benjamin E. Hermalin & Michael L. Katz, *Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy*, 4 QUANTITATIVE MKTG. & ECON. 209, 211 (2006). Traditionally, concealment is considered inefficient: "[I]t reduces the amount of information in the market, and hence the efficiency with which the market—whether the market for labor, or spouses, or friends—allocates resources." Posner, *The Economics of Privacy*, *supra* note 152, at 406. However,

information is, in general, important to reducing transaction costs (such as the ability to identify and find trading partners, settle on a price, or close the transaction), less information is broadly framed as bad or inefficient for the market.[158]

More importantly, the privacy-as-concealment construct has allowed firms to gather intimate information about consumers and then use that information to covertly undermine their decisions.[159] Recognizing privacy-as-concealment is important in order to understand the current economic anomaly where firms with interests not aligned with consumers have intimate information about those individuals. For privacy-as-concealment, disclosed information is not governed by privacy expectations since the information is no longer concealed.[160] In disclosing information, or even merely being in public or being online, consumers are seen from a legal perspective as relinquishing privacy.[161] Firms are then permitted—even expected—to gather, aggregate, sell, and use the information to create value for themselves.[162]

However, the concept of privacy-as-concealment was put forward under very specific assumptions by Posner and Stigler.[163] Their arguments presumed that information would only be shared if consumers trusted the other party and that information-sharing

---

Hermalin and Katz have found that, "(a) privacy can be efficient even when there is no "taste" for privacy *per se*, and (b) to be effective, a privacy policy may need to ban information transmission or use rather than simply assign individuals control rights to their personally identifiable data." Hermalin & Katz, *supra* note 157, at 209.

[158] The theory in economics based on the privacy-as-concealment concept by Posner and Stigler would be that privacy is equal to concealing information, and concealing information is bad for markets; therefore, privacy is bad for markets. *See generally* Posner, *The Economics of Privacy*, *supra* note 152; Stigler, *supra* note 152.

[159] *Supra* Part IV.A.

[160] *Supra* Part IV.A.

[161] *Supra* Part IV.A.

[162] *Supra* Part IV.A.

[163] *See generally* Stigler, *supra* note 152; Posner, *The Right of Privacy*, *supra* note 152.

would always be helpful to the consumer.[164] Specifically, Posner and Stigler assumed the following:

(a) Firms were assumed to never gather too much information. The cost will dissuade firms from "idly" surveilling people.[165]

(b) Data gathering, storage, and retrieval was assumed to be expensive and time consuming such that no company would store, sell, and traffic in data. Firms would always ask for information directly from the consumer.[166]

(c) Extraneous consumer information was assumed to be ignored.[167]

(d) If the collection, sharing, and use of data violated expectations or norms, the resultant cost of upsetting individuals was assumed to be felt by those firms actually gathering and

---

[164] *See generally* Stigler, *supra* note 152, at 1; Posner, *The Right of Privacy*, *supra* note 152.

[165] Posner, *The Right of Privacy, supra* note 152, at 394; Stigler, *supra* note 152, at 628–29 ("Exhaustive information costs more than it is worth; complete ignorance would make rational conduct impossible. Hence in all economic and social life, we resort to clarification.").

[166] "The storage and retrieval of information, and its accurate dissemination, are often extremely expensive, and in a vast number of situations it is much cheaper to produce the information anew rather than to seek it out." Stigler, *supra* note 152, at 625.

[167] Inappropriate information (race/sex) will not be used in decisions: "The third misuse (use of "bad" information) presents a conflict between social (majority) and individual preferences or knowledge, often with the implications that it is empirically inefficient as well as legally wrong to take the designated characteristic into account." *Id.* at 625. Posner, *The Economics of Privacy*, *supra* note 152, at 406 ("It is sometimes argued that people will misuse private information—will attach excessive weight to knowledge that a prospective employee has a criminal record, or is a homosexual, or has a history of mental illness. However, the literature on the economics of nonmarket behavior suggests that people are rational even in non-market transactions, such as marriage, and in market transactions, even in regard to such apparently emotional factors as race and sex (see, for example, Gary Becker and Edmund Phelps). Therefore, there seems to be no solid basis for questioning the competence of individuals to attach appropriate (which will often be slight) weight to private information, at least if 'appropriate' is equated with 'efficient.'").

storing the data.[168] Therefore, all collection, sharing, and use of information would be sanctioned by the empowered consumer.

Essentially, Posner and Stigler assumed that the market would fix bad behavior regarding data collection and use; if an organization collected intrusive information or collected information in a coercive manner, the affected people would walk away, and the company would have lower quality employees or no customers. Plus, economists assumed people would not reveal their information, especially if people knew their information would be used in an organization's decision that affected them.[169] Therefore, at the time, economists could assume that the interests of the individual and the firm aligned (better advertising, better product offerings, better transaction costs, etc.).[170]

These assumptions worked during the first wave of privacy scholarship in economics, when the only actor with enough money and reach to collect large amounts of information was the government.[171] However, the proliferation of data trackers and the ease, value, and cost of trafficking information now render these assumptions almost quaint. Storage, retrieval, and sharing are cheap and accurate, and data traffickers collecting and using data have no

---

[168] The requesting organization—government or private actor—will feel the market effects of requesting inappropriate information. Stigler, *supra* note 152, at 627 ("[I]t will pay for this burden through higher wage rates or lower quality employees."). If it is the state requesting inappropriate information, one can assume the state is correct in asking for it. *See id.*

[169] Farrell, *supra* note 146, at 117.

[170] *Supra* Part I.

[171] Stigler, *supra* note 152, at 623. The first assumption in this era of scholarship was that the entity that could surveil consumers was the government, the only actor with the money and reach to collect data. *Id.* ("Governments (at all levels) are now collecting information of a quantity and in a personal detail unknown in history. Consider the following: It would have been quite impossible for a public official in 1860 to learn anything about the income of a citizen chosen at random without leaving Washington, D.C. Today the files of Social Security, the Internal Revenue Service, the Securities and Exchange Commission, the microfilms of banking transactions, and other sources are potentially available to answer the question, to say nothing of the fact that perhaps one family in three or four receives payments directly or indirectly from the federal government.").

relationship with the consumer.[172] In fact, these facets of the information economy—the cheap and easy collection and storage of data and the ability to make sense of the data to target individuals—are lauded as important steps forward in the advancement of artificial intelligence ("AI") and "Big Data."[173] However, the same facets also undermine key assumptions made in putting forth the concept of privacy-as-concealment as useful or reflective of privacy expectations.[174]

B. The Reach of Privacy-as-Concealment

Yet, privacy-as-concealment still infects academic and public policy discourse and has provided the building blocks of regulatory and academic examinations of privacy.[175] Privacy-as-concealment has thus remained a force in marketing, economics, public policy, and law; privacy-as-concealment guides the generalizations drawn from surveys and the implications made for public policy and practice. For example, behavioral studies of "privacy" measure how much an individual would be willing to pay ("WTP") for privacy versus how much an individual would be willing to accept ("WTA") a privacy violation.[176] This WTA/WTP scholarship relies on privacy-as-concealment by measuring the respondents' WTP to

---

[172] *Supra* Part I.

[173] *See* Hind Benbya, Thomas H. Davenport & Stella Pachidi, *Artificial Intelligence in Organizations: Current State and Future Opportunities*, 19 MIS Q. EXEC. 9, 9 (2020); Thomas H. Davenport & Rajeev Ronanki, *Artificial Intelligence for the Real World*, 96 HARV. BUS. REV. (2018), https://hbr.org/2018/01/artificial-intelligence-for-the-real-world [https://perma.cc/Y73Z-Y6PP].

[174] *See* Varian, *Artificial Intelligence, Economics, and Industrial Organization*, *supra* note 83, at 416. Tucker also emphasizes that privacy in its modern, most used form is currently challenged for three reasons: "(1) *cheap storage* means that data may persist longer than the person who generated the data intended, (2) *non-rivalry* means that data may be repurposed for uses other than originally intended, and (3) *externalities* mean that data created by one individual may contain information about others." CATHERINE TUCKER, *Economics of Privacy and User-Generated Content*, EMERGING TRENDS IN THE SOCIAL AND BEHAVIORAL SCIENCES: AN INTERDISCIPLINARY, SEARCHABLE, AND LINKABLE RESOURCE 201 (2015).

[175] *See* Goldfarb, *supra* note 152, at 123; Acquisti, Taylor & Wagman, *supra* note 80, at 450.

[176] Angela G. Winegar & Cass R. Sunstein, *How Much is Data Privacy Worth? A Preliminary Investigation*, 42 J. CONSUMER POL'Y 425, 426 (2019).

conceal information and equating their WTP with privacy.[177] This research broadly measures consumers' valuation of "privacy" by measuring a valuation of concealment, thereby assuming that information cannot be disclosed with privacy expectations.[178] Similar measurements of privacy-concerns operationalize privacy-as-concealment, such as by assessing whether consumers reveal their income in a survey.[179] This operationalization leads academics to generalize every disclosure of information as an indication that consumers or respondents do not value privacy.[180]

This privacy paradox is perhaps the most harmful concept based on the original framing of privacy-as-concealment. The privacy paradox refers to the supposed inconsistencies between individuals' stated privacy preferences in their survey responses and their actual behavior.[181] For example, respondents indicate a concern for privacy in a survey and then researchers measure whether the respondents would disclose information online or to researchers or report to have used a social networking app.[182] Researchers can then generalize the

---

[177] Acquisti, John & Loewenstein, *supra* note 152, at 249 ("Individuals assigned markedly different values to the privacy of their data depending on (1) whether they were asked to consider how much money they would accept to disclose otherwise private information or how much they would pay to protect otherwise public information and (2) the order in which they considered different offers for their data.").

[178] Winegar & Sunstein, *supra* note 176, at 425. Alternatively, "[w]e investigate changes to the value that individuals place on the online disclosure of their private information in the presence of multiple privacy factors. We use an incentive-compatible mechanism to capture individuals' willingness-to-accept (WTA) for a privacy disclosure in a series of three randomized experiments." Joseph R. Buckman, Jesse C. Bockstedt & Matthew J. Hashim, *Relative Privacy Valuations Under Varying Disclosure Characteristics*, 30 INFO. SYS. RES. 375, 375 (2019).

[179] "[W]e measure how consumers' privacy concerns have changed using three million observations collected by a market research company from 2001-2008, covering whether consumers chose to protect their privacy by not revealing their income in an online survey." Avi Goldfarb & Catherine Tucker, *Shifts in Privacy Concerns*, 102 AM. ECON. RSCH. 349, 349 (2012).

[180] *See id.*

[181] Kirsten Martin, *Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms*, 30 BUS. ETHICS Q. 65, 65 (2020).

[182] Patricia Norberg, Daniel Horne, and David Horne, in one of the first articles naming the privacy paradox, explicitly define privacy as that which is concealed

study to posit that people claim to care about privacy but show little concern about it in their daily behavior.[183]

Importantly, the evidence of individuals not caring about privacy, or relinquishing privacy in practice, centers on individuals merely disclosing information. In a recent review of the privacy paradox as a concept, Professors Nina Gerber, Paul Gerber, and Melanie Volkamer provide examples of how individuals demonstrate their indifference to keeping their information private: "[30%] of the respondents would even trade their e-mail address for money or the chance to win a prize or be entered in a raffle and 17% are willing to give it away in exchange for access to an app."[184] Similarly, in a summary of information privacy scholarship, Professors Jeff Smith, Tamara Dinev, and Heng Xu noted the prevalence of a privacy paradox identified in research where, "despite reported high privacy concerns, consumers still readily submit their personal information in a number of circumstances."[185] The proof of (not) caring about privacy in practice is, according to privacy paradox researchers, demonstrated by consumers (not) concealing information.[186]

---

where the paradox lies in the inconsistency between respondents' intentions to disclose and their actual disclosure behavior. Patricia A. Norberg, Daniel R. Horne & David A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, 41 J. CONSUMER AFFS. 100, 100 (2007).

[183] For a summary of the definition and operationalization of the privacy paradox, see Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCI. 509, 509 (2015).

[184] Nina Gerber, Paul Gerber & Melanie Volkamer, *Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior,* 77 COMPUTS. & SEC. 226, 227 (2018) (summarizing individuals' paradoxical behavior by observing that, "[o]n the one hand, users express concerns about the handling of their personal data and report a desire to protect their data, whereas at the same time, they not only voluntarily give away these personal data by posting details of their private life in social networks or using fitness trackers and online shopping websites which include profiling functions, but also rarely make an effort to protect their data actively, for example through the deletion of cookies on a regular basis or the encryption of their e-mail communication.").

[185] H. Jeff Smith, Tamara Dinev & Heng Xu, *Information Privacy Research: An Interdisciplinary Review*, 35 MIS Q. 989, 993 (2011).

[186] *See id.*; Martin, *supra* note 181.

To explain the penchant to disclose information, scholars have linked this paradoxical behavior to the privacy calculus,[187] whereby individuals relinquish information (framed by scholars as "relinquishing privacy"[188]) in order to receive the benefits of going online. In each case of the privacy paradox or the privacy calculus, individuals are assumed to relinquish privacy upon the disclosure of information, and only information that is not disclosed is considered private.[189]

This Article argues that the privacy paradox is the most dangerous concept emanating from the privacy-as-concealment framework because this concept encourages firms to increase their collection and use of personal information without needing to worry about privacy expectations. Consumer-facing firms, marketers, and advertising advocacy groups use the privacy paradox to justify their current data practices, while also reporting data that shows consumers overwhelmingly find such practices problematic and unsettling.[190] Framing individuals as acting "paradoxically" in regard to privacy when disclosing information, going online, or

---

[187] *See* Martin, *supra* note 59, at 66 ("[F]or the privacy paradox to persist, one of two assumptions is necessary: (a) that when consumers disclose information and engage with firms, they also relinquish privacy expectations; or (b) that privacy is a preference that is easily negotiated away in the market. Philosophers and legal scholars, on the other hand, argue that reasonable privacy expectations exist post-disclosure and that privacy is a right similar to a core value to be respected at all times.").

[188] *Id. See* Gerber, Gerber & Volkamer, *supra* note 184, at 226; Paul A. Pavlou, *State of the Information Privacy Literature: Where Are We Now and Where Should We Go?*, MIS Q. 977, 979 (2011).

[189] Researchers equate the disclosure of information to "privacy-compromising behavior" in validating the privacy paradox. *See* Susanne Barth & Menno D.T. de Jong, *The Privacy Paradox–Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior–A Systematic Literature Review*, 34 TELEMATICS & INFORMATICS 1038, 1039 (2017).

[190] *See* Martin, *supra* note 59, at 65; Spyros Kokolakis, *Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon*, 64 COMPUTS. & SEC. 122, 122 (2017).

using an app relies upon a definition of privacy as only that which is concealed.[191]

C. Alternative Approaches to Privacy

Defining privacy as only that which is concealed has infected economics, public policy, social science, and legal scholarship, thereby leading scholars and practitioners to argue that individuals relinquish privacy expectations when disclosing information.[192] However, scholars have begun to focus on the privacy of revealed or public information.[193] This shift is critical, since these theories—that disclosed information retains privacy expectations—would not allow intimate knowledge of individuals' vulnerabilities to be placed in the hands of firms who can manipulate those individuals (i.e., targets).

Rather than view the disclosure of information as a signal of relinquishing privacy, more context-dependent definitions of privacy posit that the individual who shares the information does so

---

[191] In fact, the term 'paradox' is defined as "a statement that is seemingly or opposed to common sense and yet [*when investigated or explained*] is perhaps true." MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/paradox [https://perma.cc/54Y9-BKJA] (emphasis added) (last visited Dec. 21, 2021). This author thanks Alessandro Acquisti for pointing out the actual definition of paradox in reference to the privacy paradox. Many scholars have gone on to investigate this seemingly self-contradicting behavior. Often the privacy paradox is explained by countering this supposed calculus performed: Consumers cannot be expected to know or understand the privacy implications of their decision given the structure of the data markets online. *See* Waldman, *supra* note 13, at 105; Acquisti, Brandimarte & Loewenstein, *supra* note 183, at 509. In fact, contrary to the privacy paradox, consumers retain strong privacy expectations even after disclosing information. Martin, *supra* note 59, at 65. Referring to going online or using an app as somehow paradoxical in regard to privacy would be like describing women who work in companies (or universities) as falling into the discrimination paradox: They claim to not like being discriminated against yet continue to work in these organizations.

[192] *See* discussion *supra* Part IV.B.

[193] *See, e.g.*, Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 L. & PHIL. 559 (1998); Robert Gellman, *Public Records—Access, Privacy, and Public Policy: A Discussion Paper*, 12 GOV'T INFO. Q. 391 (1995); Woodrow Hartzog, *The Public Information Fallacy*, 99 B.U. L. REV. 459 (2017); Joel R. Reidenberg, *Privacy in Public*, 69 U. MIAMI L. REV. 141 (2014).

within a specific community or relationship of trust, or within a specific context of privacy norms.[194] Professor Ari Waldman offers a theory of privacy—privacy as trust—as counter to the "traditional division between public and private."[195] Within this privacy as trust theory, individuals disclose information within trust relationships—with expectations as to how their information will be shared and used.[196] Relatedly, Professors Woody Hartzog and Neil Richards conceptualize privacy as reinforcing trust within established relationships.[197] Separately, Hartzog suggests that information disclosed carries with it an understanding of confidentiality as to how that information should be used and shared, and that understanding should carry forward to all other parties who are given access to such information.[198] Each context-specific approach

---

[194] *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (Stanford Univ. Press ed., 2010); Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32 (2011); Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIAMI L. REV. 559 (2014); Richards & Hartzog, *Taking Trust Seriously in Privacy Law*, *supra* note 22; Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61 (2009); Kirsten Martin, *Understanding Privacy Online: Development of a Social Contract Approach to Privacy*, 137 J. BUS. ETHICS 551 (2016); Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 657 (2011); Daniel J. Solove, "*I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007) (carving out privacy norms around disclosed information). For more specific examples of measuring privacy norms in public, see JOSEPH TUROW ET AL., AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT, 3–4 (2009), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214 [https://perma.cc/T4N4-NYAC]); *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RSCH. CTR. (Nov. 12, 2014), https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/ [https://perma.cc/67MF-EFAS].

[195] Waldman, *supra* note 194, at 560.

[196] *Id.* at 559 ("Rather than accept the traditional division between public and private, and rather than begin and end the discussion of privacy as an individual right, this Article bridges social science and the law to argue that disclosures in contexts of trust are private.").

[197] Richards & Hartzog, *Taking Trust Seriously in Privacy Law*, *supra* note 22, at 431 ("[P]rivacy can and should be thought of as enabling trust in our essential information relationships.").

[198] Hartzog, *supra* note 194, at 659 ("A chain-link confidentiality regime would contractually link the disclosure of personal information to obligations to protect that information as it is disclosed downstream.").

governs how information should be treated post-disclosure or when not concealed.

Where Hartzog, Richards, and Waldman focus on trust as the basis for privacy expectations of disclosed information, other scholars have sought to identify specific types of disclosed information—sensitive,[199] sexual,[200] intellectual,[201] or sheer quantity[202]—as requiring privacy protection post disclosure. Professor Julie Cohen takes an alternative approach, arguing instead that the debate about data privacy protection should be grounded in an appreciation of the conditions necessary for individuals to develop and exercise autonomy and that meaningful autonomy requires a degree of freedom from monitoring, scrutiny, and categorization by others.[203] In contrast, Professor Solove proposes a taxonomy of privacy, without settling on one definition, in order to incorporate the many ways individuals have privacy expectations of both concealed and disclosed information.[204]

---

[199] Ohm, *supra* note 6, at 1128.

[200] Danielle Keats Citron, *A New Compact for Sexual Privacy*, 62 WM. & MARY L. REV. 1763, 1768 (2021) ("Sexual privacy concerns the social norms governing the management of boundaries around intimate life. It involves the extent to which others have access to and information about people's naked bodies (notably the parts of the body associated with sex and gender); their sexual desires, fantasies, and thoughts; communications related to their sex, sexuality, and gender; and intimate activities (including, but not limited, to sexual intercourse.").

[201] Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 389 (2008) ("Intellectual privacy is the ability, whether protected by law or social circumstances, to develop ideas and beliefs away from the unwanted gaze or interference of others.").

[202] David C. Gray & Danielle Keats Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 100 (2013) ("[W]e can and should maintain expectations of privacy in large quanta of personal information.").

[203] Cohen, *supra* note 20, at 1377 ("On this theory, one must, if one values the individual as an agent of self-determination and community-building, take seriously a conception of data privacy that returns control over much personal data to the individual. We must carve out protected zones of personal autonomy, so that productive expression and development can have room to flourish. We can do so—constitutionally—by creating a limited right against certain kinds of commercial collection and use of personally-identified information.").

[204] Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, *supra* note 194, at 745; Solove, *A Taxonomy of Privacy*, *supra* note 154, at 1756.

Another approach to privacy is a social contract approach, whereby individuals discriminately share information within a community with an understanding of the privacy norms governing that community.[205] Individuals reveal information with an understanding of who would be able to receive that information as well as how and why the information would be used.[206] When one talks about privacy expectations, one identifies the implicit and explicit norms about how information is expected to flow in a given community.[207]

Professor Helen Nissenbaum has been consistently (and persistently) arguing for and developing a theory of privacy in public.[208] According to Nissenbaum's theory of contextual integrity, privacy is respected when norms of appropriate information flow are respected.[209] The norms of information flow—the rules as to how information flows, to whom, and what kind of information—are dependent on the context of the information.[210] Norms of

---

[205] Martin, *Understanding Privacy Online: Development of a Social Contract Approach to Privacy*, *supra* note 194, at 551.

[206] *Id.* at 557.

[207] Contractors in all communities have rights of voice, exit, and entry, or norms are developed *as if* all contractors have rights of voice, exit, and entry. However, rights to exit and entry are macro norms; the real work of social contract theories is the identification and application of the actual privacy norms that are developed in the community.

[208] In 1998, Nissenbaum identified the problem of privacy in public: "While not denying the importance of protecting intimate and sensitive information, this paper insists that theories of privacy should also recognize the systematic relationship between privacy and information that is neither intimate nor sensitive and is drawn from public spheres." Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, *supra* note 194, at 559; Nissenbaum, *A Contextual Approach to Privacy Online*, *supra* note 195; Martin & Nissenbaum, *Privacy Interests in Public Records: An Empirical Investigation*, *supra* note 4, at 117 ("One difficulty in conceptualizing 'privacy in public' is the association of the word 'privacy' with information that is inaccessible to others. If privacy is that which is not disclosed or utterly obscure, and if public means being accessible, then something is either private or public and cannot be both. The dichotomy that follows from this—of information being secret-or-not or private-or-not—leads to the incorrect conclusion 'that there is no claim to privacy when information appears in a public record.'").

[209] *See* NISSENBAUM, *supra* note 194 at 3–4.

[210] *See id.*

information flow for education, for example, differ from norms of information flow for public health. Importantly, Nissenbaum's theory of contextual integrity is explicitly tied to the privacy of disclosed information. Rather than assume "anything goes" when information is disclosed, Nissenbaum's theory of contextual integrity identifies how individuals have reasonable expectations of privacy for disclosed information.[211] In fact, where privacy-as-concealment assumes privacy norms are not applicable for disclosed information, Nissenbaum's theory of contextual integrity really begins to hit its stride in identifying privacy norms once information is disclosed within a given context.

What justifies these privacy norms of disclosed information differs across these scholars; in fact, they do not always agree.[212] However, all argue that information is disclosed *with expectations of privacy attached* as to who will have access to the information, what uses will be appropriate, and how the information will flow. For trust-based approaches to privacy, these expectations are defined by trust between an individual and a collector of information.[213] For privacy as contextual integrity, norms of appropriate flow would dictate the expectations of information privacy based on a specific context (e.g., health care versus education versus commerce).[214] For privacy as a social contract, the expectations of privacy are the micro-norms negotiated within a defined community.[215]

---

[211] Martin & Nissenbaum, *Privacy Interests in Public Records: An Empirical Investigation*, *supra* note 4, at 121 ("One immediate consequence of defining informational privacy as contextual integrity can be observed in the approach to privacy of public data. Privacy is not lost, traded off, given away, or violated simply because control over information is ceded or because information is shared or disclosed, only if ceded or disclosed inappropriately. Releasing information is not the same as giving up privacy if the flow is appropriate.").

[212] *See, e.g.*, Kirsten Martin & Helen Nissenbaum, *Measuring Privacy: Using Context to Expose Confounding Variables*, 18 COLUM. SCI. & TECH. L. REV. 176, 176 (2017).

[213] Richards & Hartzog, *Taking Trust Seriously in Privacy Law*, *supra* note 22, at 431.

[214] NISSENBAUM, *supra* note 194, at 3–4.

[215] Kirsten Martin, *Understanding Privacy Online: Development of a Social Contract Approach to Privacy*, *supra* note 194, at 551.

This shift—from disclosed information being free from all privacy expectations to disclosed information having defined privacy expectations within a particular context, community, or relationship—is important for the governance of the flow of information that is disclosed or public. In a more recent analysis of the economics of privacy, Acquisti, Taylor, and Wagman noted that privacy is not the opposite of sharing and allowed for the possible benefits of sharing data, as well as the potential costs of sharing data with the wrong parties.[216]

When research assumes the existence of privacy expectations of disclosed information, scholars have measured how much respondents care about the privacy of their disclosed information.[217] Even in economics, when scholars have taken consumer concerns into consideration, scholars find that consumers need protection through regulations[218] or find the consumers benefit from

---

[216] Costs can range from price discrimination to other, more odious forms of discrimination; from social stigma to blackmailing; from intangible nuisances to identity theft. "Individuals can benefit from protecting the security of their data to avoid the misuse of information they share with other entities. However, they also benefit from the sharing of information with peers and third parties that results in mutually satisfactory interactions." Acquisti, Taylor & Wagman, *supra* note 80, at 462.

[217] For example, Helen Nissenbaum and this Author have measured individuals' nuanced expectations of privacy about who should collect location data or public records and how either will be used. Kirsten Martin & Helen Nissenbaum, *What Is It About Location?*, 35 BERKLEY TECH. L.J. 251, 251 (2020); Martin & Nissenbaum, *Privacy Interests in Public Records: An Empirical Investigation*, *supra* note 4, at 111. Katie Shilton's research show that individuals have strong expectations of privacy about information collected by trackers online or in apps. Katie Shilton, *Four Billion Little Brothers?: Privacy, Mobile Phones, and Ubiquitous Data Collection*, 52 COMMC'NS. ACM 48, 48 (2009). Alice Marwick and danah boyd have also shown adolescents' expectations of privacy online. Alice Marwick, *The Public Domain: Surveillance in Everyday Life*, SURVEILLANCE & SOC'Y 378, 378 (2012); Alice E. Marwick & danah boyd, *Networked Privacy: How Teenagers Negotiate Context in Social Media*, 16 NEW MEDIA & SOC'Y 1051, 1051 (2014). Karen Levy has focused on identifying privacy of individuals while working. Karen E.C. Levy, *The Contexts of Control: Information, Power, and Truck-Driving Work*, 31 INFO. SOC'Y 160, 160 (2015).

[218] Florian Hoffmann et al., *Hypertargeting, Limited Attention, and Privacy: Implications for Marketing and Campaigning* 5 (Innocenzo Gasparini Inst. for

personalized pricing[219] and promotion when given control over what data is disclosed to the targeting firm,[220] or find the seller is better off not using personalized pricing.[221] Moreover, in the criminal law context, there has been a shift to acknowledge the privacy expectations for disclosed information.[222]

In many ways, the governance of information in the commercial sphere has fallen behind other information governance areas by relying on privacy-as-concealment, thereby allowing the situation where firms have access to intimate knowledge about individuals' vulnerabilities and are able to manipulate consumers at scale. In relying on privacy-as-concealment, lawmakers and scholars were left with few reasons to regulate disclosed information and took a more libertarian—or "anything goes"—approach to public information.[223]

Econ. Rsch., Working Paper No. 479, 2013) ("[H]ypertargeting—the collection and use of personally identifiable data by firms to tailor selective disclosure—should benefit consumers when they are adequately protected by at least one of the following three conditions: their own wariness, competition, or the inability of firms to practice personalized pricing. A strong rationale for regulation emerges only when all three conditions are not met, that is, when a monopolist practices both selective communication and personalized pricing to exploit unwary consumers."); *see also* Johnson, *supra* note 95, at 128.

[219] *But see supra* Part II.C. (discussing how personalized pricing can be used to manipulate consumers in discriminatory ways).

[220] S. Nageeb Ali, Gregory Lewis & Shoshana Vasserman, *Voluntary Disclosure and Personalized Pricing* 1–2 (Nat'l Bureau of Econ. Rsch., Working Paper No. 26592, 2021). The authors examined "what happens when consumers fully control their data—not only whether they are tracked, but what specific information is disclosed to firms" and found that consumers benefit from personalized pricing when given control over what information they disclose. *Id.*

[221] "[T]he seller prefers to commit to not use information for pricing in order to encourage information disclosure. However, this commitment hurts the consumer, who could be better off by precommitting to withhold some information." Shota Ichihashi, *Online Privacy and Information Disclosure by Consumers*, 110 AM. ECON. REV. 569, 569 (2020).

[222] *See* Carpenter v. United States, 138 S. Ct. 2206, 2246, 2256 (2018) (Thomas, J., dissenting); *see id.* at 2256 (Alito, J., dissenting).

[223] Goldfarb, *supra* note 152, at 123 ("That stream of work [reliant on Posner and Stigler] emphasized the challenges in understanding reasons to regulate privacy when information flows should create efficiencies.").

V. HOW TO GOVERN MANIPULATION ONLINE

Online targeted manipulation undermines the authentic choice of consumers in the market.[224] This Article next proposes how online manipulation might be minimized and how the authentic choice of consumers, the efficiency of transactions, and the legitimacy of the market may be protected through such safeguards.

Importantly, firms are now in a position to manipulate consumers because relying on privacy-as-concealment has resulted in a more laissez-faire approach to the flow of disclosed information; information disclosed by individuals is viewed as having few rules governing whether and how the information should be shared and used.[225] Scholars have shown that the current U.S. policy, which focuses on the disclosure of information with adequate notification, does not work.[226] However, this Article argues that the disclosure of information, even with privacy notices, does not *matter* to whether privacy expectations exist. Focusing on mere

---

[224] As Posner notes, manipulation that undermines choice is regularly governed, such as when negotiating contracts under duress or undue influence or when contractors act in bad faith, opportunistically, or unconscionably. Posner, *supra* note 15, at 272.

[225] *Supra* Part IV.B.

[226] The argument that mere notification does not work has been around for years, with many attempts to have notification work better. *See generally* Lorrie Faith Cranor et al., *Are They Worth Reading? An In-Depth Analysis of Online Trackers' Privacy Policies*, 11 I/S: J.L. & POL'Y FOR INFO. SOC'Y 325 (2015); Martin, *supra* note 41; Kirsten Martin, *Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online*, 34 J. PUB. POL'Y & MKTG. 210 (2015); Kirsten Martin, *Do Privacy Notices Matter? Comparing the Impact of Violating Formal Privacy Notices and Informal Privacy Norms on Consumer Trust Online*, 45 J. LEGAL STUD. 191 (2016); Hirsch, *supra* note 24, at 439. More recently, scholars have argued for more substantive laws around privacy and information flow, seemingly giving up on notification as a useful tool. *See* Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent*, PROC. ENGAGING DATA F.: FIRST INT'L F. APPLICATION & MGMT. PERS. ELEC. INFO. 1, 1 (2009); Waldman, *supra* note 194, at 559; Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 345 (2014); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 431 (2016); Priscilla M. Regan, *A Design for Public Trustee and Privacy Protection Regulation*, 44 SETON HALL LEGIS. J. 487, 487–90 (2020).

notification is a shield for bad corporate behavior; mere notification places the onus on the consumer to make sense of an unknowable situation without any limitations on the data gathered. Further, scholars and legislators have begun designing more substantive laws about how information flows online rather than processing rules about adequate notification and choice of consumers.[227]

Governing targeted manipulation online will require placing responsibility on those in the position to manipulate rather than attempting to identify each instance of targeted manipulation. This Article makes two unique suggestions to regulate such manipulation. First, additional safeguards are needed to limit data aggregators and ad networks—specifically, any data trafficker with knowledge of individuals' vulnerabilities and without any relationship with consumers—and ensure the use of information is in the interests of the consumer. These safeguards should be enforced by external auditors. Second, consumer-facing companies should be responsible for the third parties that access their users—either for the collection of data or for the targeting of content—and ensure these third parties abide by standards of care.

A. Difficulties in Governing Manipulation

Three facets of targeted manipulation by data traffickers strain our current mechanisms governing privacy and consumer data. First, identifying manipulation is difficult not only because the actor is hidden from the target but also because, by definition, the target's decision is modified in a way that is not known to the target.[228] The difficulty in identifying manipulation from the perspective of the

---

[227] Exemplary calls have been made for more due process around consumer data-based decisions. *See generally* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93 (2014); Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. & LEE L. REV. 1 (2014). *See also* Senator Brian Schatz's proposed Data Care Act of 2018. S. 3744, 115th Cong. (2018).

[228] Wilkinson, *supra* note 13, at 345. Recall that the phenomenon of interest of this Article is targeted manipulation as the covert leveraging of a specific target's vulnerabilities to steer their decisions to the manipulator's interests.

target (or others) makes regulating specific acts or relying on consumers to identify manipulation in the market untenable.[229]

Second, the type of manipulation described herein is performed by multiple economic actors, as follows:

(1) Consumer-facing websites and apps that gain the trust of the individual;
(2) Trackers that gather the data from the websites/apps;
(3) Data aggregators and brokers who aggregate and create intimate knowledge that expose consumer vulnerabilities;
(4) Ad networks that identify potential targets and place manipulative content; and,
(5) Consumer-facing websites and apps that lure potential targets for manipulation.

Previous attempts to identify and regulate manipulation have focused only on the actors—data collectors and manipulators—that have a relationship with the target.[230] Additional pressure on consumer-facing firms is warranted but could lead to firms outsourcing bad behavior to third parties that can operate outside legal and market forces.[231] Therefore, any policy to regulate targeted manipulation needs to address each actor in its role and potential divergent interest.

Third, data traffickers—those who collect, aggregate, and sell consumer data—are the engine of the manipulation of online consumers, yet they have no interaction, contract, or agreement with

---

[229] Spencer, *supra* note 28, at 993. Spencer rightly points out the hurdles to regulating manipulation to include problems with identification, identifying causation and harm, and practical enforcement issues. *See id.*

[230] For example, solutions that focus on a fiduciary duty because of an existing relationship would not cover the work done by data aggregators, trackers, and ad networks. Balkin, *supra* note 22, at 1183; Pozen & Khan, *supra* note 42, at 497; Richards & Hartzog, *Taking Trust Seriously in Privacy Law*, *supra* note 22, at 431.

[231] *E.g.*, Michael Burgess, *Microsoft, Apple Reveal Anti-Slavery Measures in Australia Law*, BLOOMBERG NEWS (Dec. 21, 2021), https://www.bloomberg.com/news/articles/2021-12-21/microsoft-apple-suppliers-exposed-in-australia-anti-slavery-law [https://perma.cc/5YZC-ZNDY].

individuals.[232] Similarly, the United States' reliance on notice-and-choice fails to address targeted manipulation because most acts of manipulation are done by market actors without a relationship with the individual and without a legal need to notify or gain consent.[233]

B. Curtailing Manipulation Online

When manipulation is analyzed broadly, along with persuasion, nudges, and dark patterns, identifying which acts are problematic becomes difficult: "The fuzzy line between manipulation and persuasion will pose the most significant challenge to any attempt to regulate manipulation."[234] However, this Article has focused on targeted manipulation as the covert leveraging of a specific target's vulnerabilities to steer their decisions towards the manipulator's interests. Thus, targeted manipulation is positioned here as a close cousin to coercion and fraud in undermining authentic choice in the market; the phenomenon of interest is much more narrow than previous examinations of manipulation.[235]

In general, targeted manipulation can be governed by diminishing any one of the key factors of manipulation identified above: (1) aligning the interests of firms and individuals; (2) protecting the vulnerabilities of consumers; and, (3) decreasing the degree the tactic is hidden.[236] Previous governance proposals have

---

[232] As noted by Gu et al., "If data are considered the fuel of the digital economy, 'data brokers' are its catalyst." Yiquan Gu, Leonardo Madio & Carlo Reggiani, *Data Brokers Co-Opetition*, 1, 2 (CESifo, Working Paper No. 7523, 2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3343854, [https://perma.cc/3NMH-QQGN]).

[233] This limitation includes even the newer California law, called the California Consumer Privacy Act ("CCPA"), because the law's restrictions on selling to third parties do not include trackers that collect data for data traffickers. *See* 1.81.5 CAL. CIV. CODE § 1798.100 (2018).

[234] Spencer, *supra* note 28, at 985*; see also* Kilovaty, *Legally Cognizable Manipulation*, *supra* note 32, at 469; Calo, *Digital Market Manipulation*, *supra* note 8, at 1020.

[235] Calo, *Digital Market Manipulation*, *supra* note 8, at 1020; Daniel Susser, Beate Roessler, & Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, *supra* note 15, at 2; Spencer, *supra* note 28, at 984.

[236] Targeted manipulation is defined here as leveraging the vulnerabilities of individuals in order to covertly steer a target's decision towards the interests of

focused on the second and third facets—protecting vulnerabilities and decreasing the hiddenness of manipulation. These approaches are important and are discussed in detail below. However, given the economic abnormality of having an economic actor holding intimate information about an individual, this Article spends more time exploring how the interests of individuals can be aligned with those firms that collect and use their individualized data—firms without safeguards in place to align their interests with consumers, as explored above in Part III.

1. Aligning Interests

The majority of the work to manipulate goes on behind the scenes where individuals have no influence, and their interests need not be taken into account.[237] Yet, "while regulators tend to focus their efforts on primary data collectors, such as Facebook and Google, it is often the secondary use of data that lacks transparency and therefore harms the data subjects in uncontrollable ways."[238] This current approach to regulating manipulation—focusing on consumer notification and choice—provides a shield for data traffickers to collect and use individuals' data without governance.[239]

Without any market pressures, data traffickers that hold intimate knowledge of individuals should be held to a fiduciary-like standard of care regarding how individuals' data can be used. Accordingly, data traffickers would be responsible for how their products and services could be used to possibly undermine the interests of the individuals. Professor Jack Balkin and others have called for imposing fiduciary duties on firms that gather, aggregate, and use

---

the manipulator. The three facets correspond to the three components of the definition. *See supra* note 36.

[237] *See infra* Part II.B.2.

[238] Kilovaty, *Legally Cognizable Manipulation*, *supra* note 32, at 486. *See also* Hirsch, *supra* note 24, at 439.

[239] Julie Cohen, *The Inverse Relationship Between Secrecy and Privacy*, 77 SOC. RSCH.: AN INT'L Q. 883, 886 (2010) ("Most reputable firms that deal directly with consumers do disclose some information about their 'privacy practices,' but the incentive is to formulate disclosures about both purposes and potential recipients in the most general terms possible. This practice in turn shields secondary recipients of personal data, many of whom do not disclose information about their activities at all.").

individualized data,[240] such as duties of care, confidentiality, and loyalty,[241] as well as discretion, honesty, and protection.[242]

However, attempts to add information fiduciary duties to online firms have been criticized for relying on the relations of trust between consumers and firms as a basis for the obligations of care over data.[243] This circumstance has placed scholars in a bind: Relying on relationships of trust focuses on consumer-facing firms that have some data but are not the major drivers of data trafficking online. This reliance then leaves data traffickers with no obligations or duties of care since there are no relationships with consumers. Consumers are critical to most obligations of care and to fiduciary relationships because a specific harm to a consumer is the trigger for a violation, and the consumer is responsible for identifying the violation.[244] Yet, consumers are unaware of manipulation online.

This Article resolves these problems by placing a duty of care on data traffickers that is independent of any harms and of any consumer relationships. As such, internal and external auditors would enforce the principles identified in this duty of care. Further, this duty of care would hold all firms with individualized data to data integrity principles. Such companies would be required to abide by data integrity standards, similar to those of Generally Accepted

---

[240] Ian Kerr began the discussion on imposing additional duties on service providers based on their relationship with consumers. *See* Kerr, *supra* note 22, at 419. Richards and Hartzog have also consistently called for additional obligations of loyalty on firms that have an informational relationship with consumers. *See* Richards & Hartzog, *Taking Trust Seriously in Privacy Law*, *supra* note 22, at 431; Richards & Hartzog, *A Duty of Loyalty for Privacy Law*, *supra* note 22. Balkin summarizes: "Because of their special power over others and their special relationships to others, information fiduciaries have special duties to act in ways that do not harm the interests of the people whose information they collect, analyze, use, sell, and distribute." Balkin, *supra* note 22, at 1186. This is similar to Kilovaty's focus on the fiduciary duties around security breaches. *See* Kilovaty, *Legally Cognizable Manipulation*, *supra* note 32, at 457.

[241] *See* Balkin, *supra* note 22, at 1234.

[242] Balkin focuses on duties with online service providers, and Richard and Hartzog call for confidentiality to extend to online relationships; Schatz's Data Care Act is similarly situated. *See* Balkin, *supra* note 22, at 1186; Richards & Hartzog, *Taking Trust Seriously in Privacy Law*, *supra* note 22, at 431.

[243] Balkin, *supra* note 22, at 1186.

[244] *See* Tamar Frankel, *Fiduciary Law*, 71 CAL. L. REV. 795, 817 (1983).

Accounting Principles ("GAAP"), which are governed annually by a team of auditors to ensure the companies' actions are aligned with the interests of consumers about whom they hold intimate data.[245] Audits are useful to ensure companies are held to a professional standard and therefore maintain the integrity of the industry when consumers are not in a position to correct bad behavior in the market.[246] This recommendation shifts from focusing on consumers to identify transgressions, which has been shown to be burdensome or impossible given the information asymmetries,[247] to requiring internal and external governance to ensure these duties of care are respected. This recommendation would be similar to financial and accounting rules looking for insider trading and other SEC violations, which do not require a harm to determine a violation or penalty.[248]

A GAAP-like governance structure would be flexible enough to understand market needs while still being responsive to protect individual rights and concerns. And, the audit of those holding individualized data would require the firm to record and document how the firm uses that information, as well as mandate a professional data scientist to run point on the audit. These measures would pressure data aggregators to align their interests with those individuals they are targeting. The justification for adding additional safeguards to entities that hold dangerous products or place individuals in vulnerable positions is well established. For example, firms wishing to take investor money must be audited.[249] Companies involved in heavy manufacturing must abide by the U.S. Environmental Protection Agency's regulations.[250] Banks have extensive reporting requirements, which were increased in the wake

---

[245] William McGeveran calls for a GAAP-like approach for data security. *See* William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1202 (2018). Here, one would have the same idea for data protection where standards are set, and others must be certified to abide by them. *See id.*

[246] *See generally* 85 F.R. 80508 (Dec. 11, 2020).

[247] Alessandro Acquisti et al., *Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age*, 30 J. CONSUMER PSYCH. 736, 746 (2020).

[248] *See* 17 C.F.R. § 240.10b–5.

[249] *See* 12 C.F.R. § 363.

[250] *See* 15 U.S.C. 2607(a).

of the 2008 financial crisis.[251] Insurance carriers are regulated at the state level.[252] In sum, certain industries that have been shown to put individuals in vulnerable positions—where the market is unable to adequately police bad business practices—take on additional safeguards that are then continuously assessed by third parties, including government agencies and auditors.

In addition, consumer-facing firms, such as websites and apps who have a relationship with users, need to be responsible for the third parties with whom they partner and make sure their consumers' interests are respected and in alignment with all future uses of the data. Hartzog and Richards argue that "[t]he most important privacy-relevant relationships in the modern age are those between data subjects and data collectors—between humans and the companies that collect and process their information."[253] In fact, calls for fiduciary duties are based on relationships of trust and confidence with consumer-facing firms.[254]

Previously, the obligation of consumer-facing firms has focused on how those consumer-facing firms used the data they collected.[255] This Article extends the obligations identified by others to include ensuring the third parties invited to track and target consumer-facing

---

[251] *Bank Secrecy Act (BSA)*, OFF. COMPTROLLER CURRENCY, https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html [https://perma.cc/L4FW-6CND] (last visited Feb. 13, 2022).

[252] *Commercial Insurance: Regulation*, INS. INFO. INST., https://www.iii.org/publications/commercial-insurance/how-it-functions/regulation [https://perma.cc/6KLX-GA2D] (last visited Feb. 13, 2022).

[253] Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1745 (2020).

[254] Balkin, *supra* note 22, at 1223 ("By presenting themselves as trustworthy collectors and keepers of our individual data, and by emphasizing that, for reasons of security and competitiveness, they cannot be fully transparent, digital organizations induce relations of trust from us, so that we will continue to use their services.").

[255] For example, Professors Richards and Hartzog argue that firms have an obligation of loyalty if: (1) trust is invited within an informational relationship; (2) by a firm with power over an individual; (3) that has control over the consumers mediated experiences; and, (4) where the weaker party (consumer) relies on trust of that firm. Richards & Hartzog, *A Duty of Loyalty for Privacy Law*, *supra* note 22, at 52. This duty of loyalty impacts what the firm can do with the consumer's information. *Id.*

firms' users abide by the same duties of care and loyalty of the consumer-facing firms. If the first proposal above is adopted, consumer-facing firms would need to ensure all third parties pass their audit and all third parties' practices match the consumer-facing firms' obligations to their users. This obligation would prevent consumer-facing firms from outsourcing bad data practices to third parties.

Holding consumer-facing firms responsible for how their partners (third-party trackers) gather and use their users' data would be similar to calls by Richards and Hartzog to extend confidentiality of user information to new relationships (not only the consumer-facing website),[256] or McGeveran's call for collectors of consumer data to ensure third parties abide by security standards.[257] This duty would force the consumer-facing firm—with whom the individual has some influence—to make sure its users' interests are respected by the third-party trackers, ad networks, and marketers they invite to track and target their users.[258]

Holding a company responsible for their third-party relationships is not new. Professor McGeveran has called for companies to be responsible for the security of their partners within a duty of data custodians.[259] McGeveran likens the duty of security being extended to third parties to security rules under the Health Insurance Portability and Accountability Act ("HIPAA") that require a business to specify information security duties of their partners.[260] Similarly, payment card companies use contracts to

---

[256] Richards & Hartzog, *Taking Trust Seriously in Privacy Law*, *supra* note 22, at 462.

[257] McGeveran, *supra* note 245, at 1140.

[258] It is ironic that, currently, data traffickers can *sell* data to bad actors but data traffickers cannot have their data *stolen* by those same bad actors.

[259] McGeveran, *supra* note 245, at 1140. The duties "impose a special duty on these data custodians. They must dedicate systematic effort toward the safekeeping of the personal information they hold." *Id.*

[260] HIPAA established a Security Rule that requires covered businesses to "protect against any reasonably anticipated threats or hazards to the security or integrity" of information covered by the statute. 45 C.F.R. § 164.306 (2019). This Rule applies to health care providers and insurance companies, as well as any "business associates" who process the protected data for other covered businesses.

require all data custodians in their system to comply with industry data security standards.[261] Contracts like these, which impose security obligations, are enforceable in court.[262] Moreover, these companies are uniquely positioned to know which third parties they have allowed to track their users and are in the best position to enforce a contract agreement making sure those third parties abide by the above-mentioned duties of care.

In addition, consumer-facing websites and apps would be similarly responsible for what third parties (such as ad networks and marketers) are allowed to target their users with manipulative content. The consumer-facing website and apps inherently know and control which third parties use their infrastructure to target their users. Similarly, banks are required to file Suspicious Activity Reports to the Financial Crimes Enforcement Network when they suspect a third party is using their infrastructure for money laundering or fraud.[263] One can also look closer to home. Most universities have extensive agreements managing the actions of third-party recruiters invited onto campus to hire their students.[264] Just as universities owe a duty of care to students when allowing third parties on campus, websites and apps would likewise have a duty of care to protect individuals from third parties whose interests may not align with the users.[265]

Id. HIPAA further requires a covered business to specify the security duties of their business associates in written contracts. *See id.*

[261] McGeveran, *supra* note 245, at 1166.

[262] *Id.* at 1175.

[263] These financial institutions will monitor employees to check for insider activity and will track customer transactions to check for evidence of money laundering or fraud. *What Is a Suspicious Activity Report?*, THOMSON REUTERS, https://legal.thomsonreuters.com/en/insights/articles/what-is-a-suspicious-activity-report (last visited Feb. 10, 2022) [https://perma.cc/B588-UVA8].

[264] *See, e.g.*, *Recruiting and Offer Info*, UNIV. MICH. CAREER CTR., https://careercenter.umich.edu/content/recruiting-and-offer-info (last visited Feb. 10, 2022) [https://perma.cc/54J4-4XNF] ("All employers utilizing our online posting system, Handshake, for posting positions, on-campus interviews, and other related recruitment activities will be asked to read and agree to our Recruiting Policy below.").

[265] Trademark law provides another example of a company being responsible for the questionable behavior of their third-party partners. A defendant can be

Typically, consumer-facing firms act as a "honeypot" by luring in consumers under the auspices of a trusting relationship only to then allow third parties to track the users and sell their information to data traffickers, and then later maintain user engagement for data traffickers to manipulate a target covertly. Put this way, not enough attention has been focused on the role of consumer-facing firms in choosing the third parties that track and target their users. In fact, focusing primarily on consumer-facing firms' data practices allows these firms to outsource their bad data practices to ungoverned third parties operating outside the reach of market or regulatory forces.[266]

Importantly, this approach to align interests rather than limit the use of data avoids two persistent problems in regulating information flow online. First, attempts to limit the use of data run into First Amendment critiques.[267] If the flow of information is taken as a given or legitimate, regulators have an uphill battle limiting what a company can say (a type of "use") with that data.[268] Second, designating a use as "unfair" usually relies on a *discernable harm* to the consumer in order to trigger a regulation or law,[269] such as the

---

indirectly liable for trademark infringement if the defendant: (1) "intentionally induces another to infringe" or (2) "continues to supply its product to one whom it knows or has reason to know is engaging in trademark infringement." Inwood Labs, Inc. v. Ives Labs, Inc., 456 U.S. 844, 854 (1982). Large service providers, such as eBay, must have more than just general knowledge that its service is being used to infringe, but the service provider cannot be willfully blind. Tiffany (NJ) Inc. v. eBay, Inc., 600 F.3d 93, 110 (2d Cir. 2010), cert. denied, 562 U.S. 1082 (2010). This principle would mean that ignoring the questionable behavior of partners *on purpose* is not a legitimate defense.

[266] The outsourcing of bad business practices has a long history. Garment and manufacturing companies can outsource poor labor practices to other countries. Outsourcing need not be to other countries; e.g., a manufacturer may build in a non-union state to avoid union rules, or retailers may outsource cleaning staff and maintain plausible deniability as to the poor labor practices.

[267] Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 57 (2014); Jane R. Bambauer, *The Relationships Between Speech and Conduct*, 49 U.C. DAVIS L. REV. 16, 16 (2016).

[268] Ashutosh Bhagwat, Sorrell v. IMS Health*: Details, Detailing, and the Death of Privacy*, 36 VT. L. REV. 855, 855 (2011); Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1501 (2015).

[269] Calo, *supra* note 8, at 995.

Federal Trade Commission's ("FTC's") unfairness doctrine,[270] the unfairness protections of consumer protection laws,[271] or even in a recently proposed Data Protection Act.[272] But the harms from manipulation are not the kind normally identified by regulators, or the harms are so dispersed as to be difficult to identify; and therefore, the traditional triggers of data regulation fail to protect consumers online.[273] Accordingly, the approach proposed in this Article does not rely on a consumer to identify a specific harm to trigger an investigation into problematic use of data.[274]

2. Protecting Vulnerabilities

Another mechanism to regulate manipulation is to limit firms' collection and use of intimate knowledge, effectively protecting consumers' vulnerabilities. Manipulation is only possible because someone—here, a data broker—has intimate information of individuals and knows what renders them vulnerable in their decision-making. A number of scholars have proposed greater protections on specific types of data, such as intimate data,

---

[270] 15 U.S.C. § 45(a)(1) (2012).

[271] Federal Trade Commission (FTC) Act of 1914 § 5, 15 U.S.C. § 45 (2012).

[272] Hirsch, *supra* note 24, at 439; Kilovaty, *supra* note 32, at 486; Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2235–36 (2015); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 598–606 (2014); *see* Data Protection Act, S. 3300, 116th Cong. (2020).

[273] Calo, *supra* note 8, at 995; Kilovaty, *supra* note 32, at 450.

[274] Others leave open the idea that the FTC could regulate data practices based on procedural issues, such as Citron and Pasquale. Citron & Pasquale, *supra* note 227, at 1. Hirsch sees the unfairness doctrine as requiring an "injury," which, as noted by Calo, does not usually cover the type of injury to the market described herein—however, perhaps in the future. Hirsch, *supra* note 24, at 481 ("This language creates a three-prong test. In order to exercise its unfairness authority the FTC must first demonstrate that: (1) the business act or practice in question causes 'substantial injury to consumers'; (2) consumers themselves cannot 'reasonably avoid[]' this injury; and (3) the consumer injury that the business practice creates is 'not outweighed' by its 'benefits to consumers or to competition.'").

inferences drawn from data,[275] and sensitive information.[276] Professor Dennis Hirsch broadens what could constitute "vulnerable" in noting that surface information becomes problematic through predictive analytics.[277] Hirsch has advocated for curtailing the collection of information at the source with the idea that the consumer data that is not collected cannot also be used against the consumers.[278] Others have focused on limiting the use of information once collected and have attempted to identify problematic instances of use, such as unfair practices, unreasonable self-dealing, and breaches of loyalty and confidentiality.[279]

3. Eliminating Hiddenness

Another way to undermine the effectiveness of manipulation is to make obvious and public the type of intimate knowledge used in targeting, thereby eliminating the component of manipulation that makes manipulation effective: hiddenness. Manipulation works because the tactic is hidden from the target. However, notification requirements are rarely an effective regulatory regime as companies have no substantive requirements as to what their notifications must entail. To be effective, a notice must be specific as to the vulnerability being leveraged in a manipulative ad (e.g., "We placed this ad because we think you are a gambler"). In addition, a registry could serve as a notification to regulators and researchers as to the type of information used to hyper-target users, whereby researchers can retroactively identify the major factors used to target.

C. Specific Policy Suggestions Across Regulations

The suggested regulatory mechanisms above would entail a new governance structure to ensure data traffickers safeguard individualized data and align their interests with consumers. To

---

[275] Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 COLUM. BUS. L. REV. 494, 494 (2019).

[276] Ohm, *supra* note 6, at 1125.

[277] Hirsch, *supra* note 24, at 439.

[278] Susser, Roessler & Nissenbaum, *supra* note 15, at 12.

[279] Hirsch, *supra* note 24, at 464–68; Balkin, *supra* note 22, at 1183; Hartzog & Richards, *supra* note 253, at 1750–52; Eliza Mik, *The Erosion of Autonomy in Online Consumer Transactions*, 8 L. INNOVATION & TECH. 1, 4–6 (2016).

enforce new privacy regulations, some call for expanding the FTC's current scope of authority,[280] while Professor Priscilla Regan calls for a new regulatory agency within the U.S. Department of Commerce.[281]

Nevertheless, across privacy regulations, the following steps can be taken that would make targeted manipulation less likely. First, regulations should explicitly recognize individual autonomy—defined as the ability of individuals to be the authentic authors of their own decisions—as a human right in order to protect individuals from manipulation done in the name of "legitimate interests" within the G20's AI Principles and within the European Union's General Data Protection Regulation.[282] For example, an individual has a right to the restriction of information-processing dependent on the legitimate grounds of the controller.[283] Yet, "legitimate interests" are broadly construed and the manipulation of individuals has not been identified as diminishing a human right.[284] One fix is to more clearly link manipulation to individual autonomy, which would be seen as a human right that could trump even the legitimate interests of data traffickers.[285]

Second, all regulators should expand the types of information requiring additional safeguards to protect users' vulnerabilities from being used for manipulation. Specifically, "inferences" should be included as a type of protected data. The inferences made by data traffickers based on a mosaic of information about individuals can constitute intimate knowledge as to who is vulnerable and when. Current approaches only include collected data as protected rather

---

[280] Solove & Hartzog, *supra* note 272, at 585–87; Hirsch, *supra* note 24, at 451.

[281] Regan, *supra* note 226, at 504.

[282] Council Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 and on the protection of natural persons with regard to processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) at art. 14 (EU).

[283] *Id.* at art. 14(2).

[284] G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948).

[285] Zarsky rightly notes that threats to autonomy undermine at the level of the individual and society. Tal Z. Zarsky, "*Mine Your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, 5 YALE J.L. & TECH. 1, 38–40 (2002).

than the inferences drawn about individuals based on that collected data.[286]

Finally, all regulations should expand the definition of "sold data" to make sure all regulations include beacons and tracking companies in the requirement to notify if user data is "sold." The California Consumer Privacy Act ("CCPA") has restrictions on selling to third parties but does not include trackers who collect data for data traffickers.[287] Additionally, "the CCPA requires a business to provide notice if it is 'collect[ing] personal information collected for additional purposes.' This rule on its face does not stop companies from using data for new purposes—it just requires disclosure if they do so."[288] The approach to regulating manipulation generally and within specific sectors would seek to diminish the key facets of manipulation identified above: (1) aligning the interests of firms and individuals; (2) protecting the vulnerabilities of consumers; and, (3) decreasing the degree the tactic is hidden.

VI. CONCLUSION

In sum, this Article starts with the economic abnormality of firms in the position to leverage individuals' vulnerabilities to manipulate consumers and then explores how firms gained the power and knowledge to manipulate indiscriminately without regulatory or market oversight. Firms in a position to leverage aggregated consumer data is a symptom of the mistaken framing of privacy-as-concealment in law, economics, and public policy. Where scholarship has focused on identifying instances of manipulation to regulate, this Article argues that firms *merely in the position* to manipulate, with the intimate knowledge of the individual and access to their decision-making, should be regulated to ensure their interests are aligned with the target.

Governing targeted manipulation online will require additional safeguards on those firms in a position to manipulate rather than

---

[286] Hirsch, *supra* note 24, at 450–52; Wachter & Mittelstadt, *supra* note 275, at 513–14.

[287] *See* 1.81.5 CAL. CIV. CODE § 1798.100, *supra* note 233.

[288] Anupam Chandler et al., *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1757 (2021).

attempting to identify each instance of targeted manipulation. First, additional safeguards limiting data aggregators and ad networks—specifically, any data trafficker without any relationship with consumers—are needed to ensure the use of information is in the interests of the consumer. Second, consumer-facing websites and apps act as gatekeepers by luring in consumers to have their data tracked by third parties and later targeting customers with manipulative content. In so doing, consumer-facing companies should be responsible for ensuring all third parties that access their users—either for data collection or for targeting content—abide by standards of care that are audited.