MANIPULATION, PRIVACY, AND CHOICE

DRAFT – PLEASE CONTACT AUTHOR BEFORE CITING.

Kirsten Martin[*]

SUMMARY

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 in order 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.

The phenomenon of interest in this article is targeted manipulation as the covert leveraging of a specific target's vulnerabilities to steer their decisions to the manipulator's interests. I position online targeted manipulation as undermining the core economic assumptions of authentic choice in the market. I then explore 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 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.

The goal of this paper is to argue 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 their interests are aligned with

[*] Kirsten Martin, PhD is the William P. and Hazel B. White 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, XXXX, 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.

the target. The economic oddity is not that firms have data that render another market actor vulnerable, 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. Online, companies have collected preferences and concerns without such safeguards in place.

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 – rather than harms to the consumer – 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 limiting 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. These obligations of care do not rely on any harm to be quantified or for a consumer to negotiate or enforce the obligation. Instead, internal and external governance structures will be required to ensure the duty of care is enforced including external auditing to ensure the data trafficker abides by standards of care and data integrity.

Second, customer facing websites and apps act as gatekeepers by luring consumers in 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 to ensure all third parties that access their users – either for the collection of data or for the targeting of content – abide by a standards of care that are audited. Companies are regularly held responsible for how third parties treat their customers, users, or employees; and, websites and apps should be held responsible for the third party ad networks, trackers, and data traffickers they invite to surveille and manipulate their users. Where scholarship has focused on identifying instances of manipulation to regulate, I argue 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

I. INTRODUCTION

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

> *Data broker Acxiom provides up to 3,000 attributes and scores on 700 million people including purchases, net worth, likelihood someone is having a baby or adopting a child, and their health interests.*[2]

Data brokers proudly collect information on millions of individuals with thousands of data points on each target. 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 if someone is depressed, anorexic, addicted to drugs or alcohol, or has a medical condition. 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.[3] Paul Ohm succinctly summarizes, "[companies] hoard this data for future, undefined uses; redistribute it to countless third parties; and repurpose it in ways their customers never imagined." [4]

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.[5] I call this targeted manipulation, which is the covert leveraging about a specific target's vulnerabilities to steer their decision to the manipulator's interest. As Ryan Calo predicted in one of the first papers on manipulation of consumers online, hyper-targeting combined with the data

---

[1] George J Stigler, "The Economics of Information," *Journal of Political Economy* 69, no. 3 (1961): 213–25, 213.

[2] https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information

[3] https://www.wordstream.com/blog/ws/2017/06/27/most-expensive-keywords
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 "Pest control" at #20

[4] Paul Ohm, "Sensitive Information," *Southern California Law Review* 88 (2015): 1125-1196, 1128.

[5] As an example, companies can morph a target's face with a model for advertising. Such face-morphs are thought to be more trusting that a stranger, however initial experiments have not shown this to impact behavior. Sonam Samat, Eyal Peer, and Alessandro Acquisti, "Can Digital Face-Morphs Influence Attitudes and Online Behaviors?," 2018, 117–25.

collected on individuals could allow firms to predict moods, personality, stress levels, health issues, etc., and potentially use that information to undermine the decisions of consumers.[6] In fact, Facebook offered advertisers the ability to targets teens when they are "psychologically vulnerable."[7] Data aggregators, data brokers, ad networks and other types of "data traffickers"[8] can not only predict what we want and how badly we need it, but can also leverage knowledge about an individual's vulnerabilities to steer his or her decisions in the interest of the firm.

Recent examinations of online consumer manipulation have defined manipulation broadly as to include standard persuasion and advertising tactics[9] or have centered on the use of human psychology to prime market decisions across consumers (e.g., nudging or dark patterns).[10] Folding targeted manipulation within persuasion or nudging allows a tactic, which is closer to fraud or coercion in undermining choice in the market, to hide with 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 to the manipulator's interests.

---

[6] Ryan Calo, "Digital Market Manipulation.," *George Washington Law Review* 82, no. 4 (2014): 995-1051. Tal Zarsky was one of the first to identify manipulation online as problematic. Tal Z Zarsky, "Online Privacy, Tailoring, and Persuasion," in *Privacy and Technologies of Identity* (Springer, 2006), 209–24.

[7] Nitasha Tiku, Get Ready for the Next Big Privacy Backlash Against Facebook, WIRED.COM, May 21, 2017,

[8] Professor Lauren Scholz uses the term 'data traffickers' to include companies who traffic in consumer data behind the scenes and without the knowledge of the consumer Lauren Henry Scholz, "Privacy Remedies," *Indiana Law Journal*, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3159746.. I use this term throughout to mean any company with individualized data without a relationship with users or customers. These companies make their money trafficking consumer data.

[9] Cass R Sunstein, "Fifty Shades of Manipulation," *Journal of Marketing Behavior* 1, no. 3–4 (2016): 213–44.

[10] See also Shmuel I Becher and Yuval Feldman, "Manipulating, Fast and Slow: The Law of Non-Verbal Market Manipulations," *Cardozo L. Rev.* 38 (2016): 459; T Martin Wilkinson, "Nudging and Manipulation," *Political Studies* 61, no. 2 (2013): 341–55; Anne Barnhill, "I'd like to Teach the World to Think: Commercial Advertising and Manipulation," *Journal of Marketing Behavior* 1, no. 3–4 (2016): 307–28; Arvind Narayanan et al., "Dark Patterns: Past, Present, and Future," *Queue* 18, no. 2 (2020): 67–92; Ari Ezra Waldman, "Cognitive Biases, Dark Patterns, and the 'Privacy Paradox,'" *Current Opinion in Psychology* 31 (2020): 105–9. Acquisti et al summarize the research on nudges in regards to privacy in Alessandro Acquisti et al., "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online," *ACM Computing Surveys (CSUR)* 50, no. 3 (2017): 1–41..

In doing so, I move away from broader interpretations of manipulation centered on irrational decisions, nudges, and persuasion, which render manipulation so pervasive to be un-governable. I focus 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.[11] Targeted manipulation defined here has three important facets: the exploitation of an individual's vulnerabilities, the covertness of tactic, and the divergence of interests between manipulator and target.

More specifically, this conceptualization focuses on manipulation as undermining an individual's ability to enact their preferences through choice. We generally seek to preserve choice in the market, where consumer choice is meaningful and indicative of consent to the transaction. Preserving choice-as-an-indicator-of-consent is not only critical for autonomy and a robust political society, it is a fundamental assumption in economics and business as to the efficiency of transactions and the legitimacy of markets. As such, I position manipulation is 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.

The goal of this paper is to argue 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. In other areas, when someone is in a position to manipulate—in a position to exploit the relative vulnerabilities or weaknesses of a target in order to usurp their decision making—safeguards force their interests to be aligned and punishes acts that are seen as out of alignment of the target. 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, I will then ask: *how did firms gain positions of power to exploit vulnerabilities and weaknesses of individuals without the requisite safeguards in place?* I argue this current

[11] Daniel Susser, Beate Roessler, and Helen Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World," *Available at SSRN 3306006*, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3306006; Joseph Raz, *The Morality of Freedom* (Clarendon Press, 1986); Eric A Posner, "The Law, Economics, and Psychology of Manipulation," *Journal of Marketing Behavior* 1, no. 3–4 (2016): 267–82.

market problem—where firms, whose interests do not align with consumers, have the knowledge and position to manipulate consumers—is due to the incorrect framing of privacy as relinquished upon disclosure in economics and law.[12]

Governing targeted manipulation online will require placing responsibility on those in the position manipulate rather than attempting to identify each instance of targeted manipulation. I make two unique suggestions in the last section. 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 the use of information is not used to manipulate consumers. This will entail data integrity principles that are enforced through auditing by third parties. Importantly, these obligations of care do not rely on any harm to be quantified, an established consumer relationship, or for a consumer to enforce the obligation. Data traffickers – companies that collect, store, process, individualized data -- would be subject to annual audits similar to other industries requiring public trust but not regulated by the market (e.g., banks, accounting in firms, environmental impact for manufacturing).

Second, I also argue that 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 a standards of care and are audited. Consumer facing websites and apps lure consumers so that their data is collected and later used against them and should be held responsible for the third parties they invite to track and target their users. Current solutions[13] place a duty of care or

---

[12] This article does not cover the harm from the individual being surveilled. That is not meant to diminish the ethical implications of surveillance, only to narrow the scope of the article. For example, respondents find being surveilled while forming preferences to undermine their autonomy. Yonat Zwebner and Rom Y Schrift, "On My Own: The Aversion to Being Observed During the Preference-Construction Stage," *Journal of Consumer Research*, 2020; Julie E Cohen, "Privacy, Visibility, Transparency, and Exposure," *The University of Chicago Law Review*, 2008, 181–201; Julie E Cohen, "Examined Lives: Informational Privacy and the Subject as Object," *Stanford Law Review*, 2000, 1373–1438; Julie E Cohen, "Turning Privacy inside Out," *Theoretical Inquiries in Law* 20, no. 1 (2019): 1–32. Professor Neil Richards defends intellectual privacy as the ability to develop ideas and beliefs away from an unwanted gaze.

[13] Ian R Kerr, "The Legal Relationship between Online Service Providers and Users," *Can. Bus. LJ* 35 (2001): 419; Jack M Balkin, "Information Fiduciaries and the First Amendment," *UCDL Rev.* 49 (2015): 1183; Ariel Dobkin, "Information Fiduciaries in Practice: Data Privacy and User Expectations," *Berkeley Tech. LJ* 33 (2018): 1; Neil M

loyalty on consumer facing firms, which can create pressure for these firms to then outsource bad privacy practices to third parties. This article offers a complementary solution to whose arguing for duties of loyalty and care for consumer facing firms by (1) extending the duties of consumer facing firms to include a responsibility for the third parties they invite to track and target their users and (2) by placing additional safeguards (an audit) on data traffickers in a position to manipulate consumers but outside the reach of current regulations and proposed legal solutions as well as outside any market pressures.

In sum, this paper starts with the economic abnormality of firms in the position to leverage knowledge of individuals' vulnerabilities to manipulate consumers and then explores how firms gained the power and knowledge to manipulate indiscriminately without regulatory or market oversight. 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. Where scholarship has focused on identifying instances of manipulation to regulate, I argue that firms merely in the position to manipulate, with the knowledge of the individual's vulnerabilities and access to their decision making, should be regulated to ensure their interests are aligned with the target.

Richards and Woodrow Hartzog, "Taking Trust Seriously in Privacy Law," *Stan. Tech. L. Rev.* 19 (2016): 431–72; Neil M Richards and Woodrow Hartzog, "A Duty of Loyalty for Privacy Law," *Available at SSRN*, 2020.

II. MANIPULATION AND THE PHENOMENON OF INTEREST

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.[14] These vulnerabilities are identified through the broad collection of data across websites, apps, and technologies and then collecting search terms, contacts, locations, and browsing histories. Such "surface data" can be used to "infer latent, far more sensitive data about" individuals through predictive analytics.[15] Ryan Calo summarizes, "the 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."[16] The knowledge of individuals' vulnerabilities can be tracked directly—through search queries for gambling or medical symptoms or teenage depression, for example—or via inferences drawn from the vast surface data, almost always when the consumer is not aware. 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, physical movement"[17] allow for dynamic emotional targeting or psychographic targeting.[18]

---

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

[15] Dennis D Hirsch, "From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics," *Md. L. Rev.* 79 (2019): 439, 439. As Ohm and Peppet note, everything can reveal everything (xxxx).

[16] Calo, "Digital Market Manipulation." 1030

[17] Shaun B Spencer, "The Problem of Online Manipulation," *Available at SSRN 3341653*, 2019. 979. E.g. IBM has filed a patent for a process that helps search engines "return web results based on the user's 'current emotional state,'" based on indicia of mood drawn from webcam facial recognition, a scan of the user's heart rate, and even the "user's brain waves."156 Sidney Fussell, "Alexa Wants to Know How You're Feeling Today," The Atlantic, October 12, 2018, https://www.theatlantic.com/technology/archive/2018/10/alexa-emotion-detection-ai-surveillance/572884/.

[18] Burkell and Regan provide an excellent example leveraging the morphing of two faces (one being the target) into one person used in advertising. Jacquelyn Burkell and Priscilla M Regan, "Voter Preferences, Voter Manipulation, Voter Analytics: Policy Options for Less Surveillance and More Autonomy," *Internet Policy Review* 8, no. 4 (2019). Such tactics are

Targeted manipulation is fueled by both this knowledge of individuals' vulnerabilities and also 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.[19] In other words, targeting a consumer based on broad demographics—e.g., for being a 50-year old male—is not as useful 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 presidential campaign relied on very specific ads being seen by only people who may be swayed by them and not seen by people who may be able to call out the inaccuracies. Manipulation would "affect a person's thoughts, opinions, and actions," and it is targeted to exploit specific vulnerability of the target.[20]

Previous examinations have pooled together the targeted manipulation, which is the phenomenon of interest here, with broader attempts to steer consumers and users such as the use of dark patterns and nudges.[21] This is

---

used in commercial and political advertising Daniel Susser, Beate Roessler, and Helen Nissenbaum, "Technology, Autonomy, and Manipulation," *Internet Policy Review* 8, no. 2 (2019); Calo, "Digital Market Manipulation."; Burkell and Regan, "Voter Preferences, Voter Manipulation, Voter Analytics: Policy Options for Less Surveillance and More Autonomy"; Ira S Rubinstein, "Voter Privacy in the Age of Big Data," *Wis. L. Rev.*, 2014, 861; Frederik J Zuiderveen Borgesius et al., "Online Political Microtargeting: Promises and Threats for Democracy," *Utrecht Law Review* 14, no. 1 (2018): 82–96.. However, there may be limits as to the effectiveness at the individual level given current abilities Samat, Peer, and Acquisti, "Can Digital Face-Morphs Influence Attitudes and Online Behaviors?"

[19] This 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 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 (CITE).

[20] "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," *Berkeley Technology Law Journal*, 2019. 449

[21] Acquisti et al., "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online."Arunesh Mathur et al., "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites," *Proceedings of the ACM on Human-Computer Interaction* 3, no. CSCW (2019): 1–32; Narayanan et al., "Dark Patterns: Past, Present, and Future"; Waldman, "Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'"; Cass R Sunstein, "Nudges Do Not Undermine Human Agency," *Journal of Consumer Policy* 38, no. 3 (2015): 207–10. As a caveat to this statement, nudges and dark patterns that are based on individualized

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 target's decisions, get lost in a larger examination of broader tactics.[22] This article remains focused on the phenomenon of interest—targeted manipulation online—but does not examine broader attempts to change behavior online such as with nudges and dark patterns. [23]

B. Necessary Components of Manipulation

Such 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 in an established relationship where the manipulator comes to know the vulnerabilities and weaknesses of the target and is in a position to covertly undermining 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 their interests. Similarly, a caregiver knows the vulnerabilities of their charge (a toddler, a patient, etc.) and is close enough to be able to manipulate their decisions away from the interest of the charge and towards the interest of the caregiver.

Targeted manipulation defined here[24] has three important facets: the exploitation of an individual's vulnerabilities, the covertness of tactic, and

---

vulnerabilities and targeting 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.Logan Warberg, Alessandro Acquisti, and Douglas Sicker, "Can Privacy Nudges Be Tailored to Individuals' Decision Making and Personality Traits?," 2019, 175–97.

[22] This article also does not explicitly cover the issues around gamification or addictive designs which are also important attempts to modify consumer behavior broadly. Tae Wan Kim and Kevin Werbach, "More than Just a Game: Ethical Issues in Gamification," *Ethics and Information Technology* 18, no. 2 (2016): 157–73.

[23] This is picking up the first argument of Ryan Calo's seminal article "The first is that the digitization of commerce dramatically alters the capacity of firms to influence consumers at a personal level." Professor Calo goes on to also include broader attempts to sway decisions online such as the use of biases and nudges. However, I will remain on the targeted manipulation he first brought up in Calo, "Digital Market Manipulation."

[24] Targeted manipulation is defined here as leveraging the vulnerabilities of individuals

the divergence of interests between manipulator and target. I explore each below and explain why each facet separates this examination from previous work on online manipulation.

1. Exploiting an individual's specific weaknesses or vulnerabilities

Key to manipulation is the leveraging of weaknesses or vulnerabilities of an individual 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, based on the targets' lack of knowledge and lack of experience. But manipulation can also be based on a relative position of power and unique knowledge about the target.

Online, 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.[25] These companies collect "surface data"[26] to predict if someone is depressed, anorexic, addicted to drugs or alcohol, or has a medical condition and then link that information to where they are, what decisions you may be making, and where you may go next.[27] Ad networks and advertisers use this information and are willing to pay top dollar to identify those in financial and emotional difficulty to promote gambling, cures, rehab, and payday loans.[28]

---

in order to covertly steer a target's decision towards the interests of the manipulator. The three facets correspond to the three components of the definition.

[25] Calo's focus was more general than mine here: with the ability to influence consumers by exploiting their tendency to act with biases or "irrationally." Calo, "Digital Market Manipulation."

[26] Hirsch notes that the more innocuous data we shed when online (e.g., like the purchase of furniture anti-scuff pads" p. 456) can be analyzed with predictive analytics to identify latent knowledge ("like credit card default risk" p. 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." P. 442. Hirsch, "From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics."

[27] Zwebner and Schrift, "On My Own: The Aversion to Being Observed During the Preference-Construction Stage."

[28] https://www.wordstream.com/blog/ws/2017/06/27/most-expensive-keywords

Firms, platforms and other data aggregators are also in a structural position of power over their users both because they retain unique services or knowledge that the individual is seeking and because they are in a position of power via information asymmetry where the user is unable to fully know what is going on with their data. The individual is in a position of vulnerability vis-à-vis the data controller.[29] While anyone can commit fraud or deceive, manipulation requires a power or knowledge imbalance rendering the target vulnerable to exploitation. The target can either be in a perennial vulnerable state, such as a child with an adult, or be in a temporary vulnerable state, such as when a client provided details to a lawyer, therapist, or doctor or when a company provides concerns, preferences, and forecasts to a third party.[30]

2. Being Hidden

Manipulation works because it is covert and hidden from the target.[31] The target must be unaware of the tactic being used in order to be effective. According to Susser et al.:

> manipulative 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.

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 could be used. Covertness in manipulation is necessary because the target would never endorse the tactic if it was known. Second

---

Examples of keywords related to urgent problems include: "Bail bonds" at #2"Lawyer" at #4 "Cash services & payday loans" at #7 "Rehab" at #11 "Plumber" at #18 "Termites" at #19 "Pest control" at #20

[29] Lina M Khan and David E Pozen, "A Skeptical View of Information Fiduciaries," *Harv. L. Rev.* 133 (2019): 497.

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

[31] Manipulation is "power exercised deceptively" Robert Goodin 1980. As noted by Alan Ware (1981" A has manipulated B: "B either has no. knowledge of, or does not understand, the ways in which A affects his choices" p. 165

the hiddenness renders the manipulation harder to combat, identify, and regulate**.** The hiddenness is so important to manipulation that Ryan Calo suggests disclosure would minimize the harm or power of manipulation: if "manipulation subjects are informed, the potency of manipulation may be weakened."[32] 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 be able to walk away or counter the manipulation.

The hiddenness differentiates manipulation from mere persuasion.[33] Persuasion works because the tactic is known by the target, whereas manipulation works only if the tactics are hidden. In fact, manipulation is necessary when direct, open appeals to the preferences of the target do not work. 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 with cogent (or not so cogent) arguments. In this way, manipulation starts where persuasion ends—where the manipulator ceases to engage openly with the target in a way that the target could counter. Persuasion is engaging in the marketplace of ideas by being open and subject to counter arguments.[34] Targeted manipulation circumvents the marketplace of ideas by being hidden.

In fact, conflating manipulation with persuasion makes manipulation harmless and omnipresent. Sunstein defines manipulation as a form of persuasion and then summarizes, *"*the problem is that as defined here*,* manipulation can plausibly be said to be pervasive. It can be found on

---

[32] Kilovaty, "Legally Cognizable Manipulation," 2019. 462

[33] An alternative view is that manipulation is just unseemly persuasion. Zarsky defines it as "a process in which forms 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," *Theoretical Inquiries in Law* 20, no. 1 (2019): 157–88, 157. He notes that this is a broad issue: "Striving to manipulate and exert influence is, of course, not new. Quite to the contrary, almost every form of human communication tries to do so" Zarsky 170. See also Barnill who uses examples such as nudging or priming as well as simple print advertising and persuasion in the analysis of manipulation Barnhill, "I'd like to Teach the World to Think: Commercial Advertising and Manipulation.". By broadening the phenomenon of interest to include persuasion (e.g. Zarsky) and nudges (Barnill) the problematic tactic of targeted manipulation is able to hide amongst the less problematic and harder to govern tactics of nudges and persuasion.

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

television, on the Internet, in every political campaign, in countless markets, in friendships, and in family life."[35] Defenders of manipulation in economics, marketing, or practice broaden the definition to include persuasion and advertising, thereby rendering the definition of manipulation so broad as to include legitimate acts – and making the act impossible to regulate.[36]

3. Undermining the interests of target

Finally, the goal of manipulation is to prevent the target from pursuing their own interests and to "promote the outcome sought by the manipulator."[37] 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 go outside with clothes on). Online, firms can leverage a consumer's known vulnerabilities—addiction to gambling, concern for a family member's depression, a pending divorce—to shift their decision from their current interests towards the firms' interests**.** This approach, which focuses on the divergence of interests. leaves open the possibility that manipulation could be within societal norms, an ethic of care, and respect for human dignity.[38] As Professor Kilovaty summarizes, "Manipulation by itself is not an absolute evil. Rather, it depends on whether

---

[35] Sunstein, "Fifty Shades of Manipulation." 8

[36] E.g., "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." Eldar Shafir, "Manipulated as a Way of Life," *Journal of Marketing Behavior* 1, no. 3–4 (2016): 245–60, 245. Sher (2011, p. 97) 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 also Vance Packard, The Hidden Persuaders (1957) or John Kenneth Galbraith, The Affluent Society 155–56 (1958). 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.

[37] Allen Wood, "Coercion, Manipulation, Exploitation," *Manipulation: Theory and Practice*, 2014, 17–50, 31. Wood. suggests that different tactics could be seen as manipulative—even within the definition of covertly undermining a target's decisions making towards the manipulator's interests—such as lying, misleading, encouraging false assumptions, and fostering self-deception. Here, I focus on the leveraging of vulnerabilities which could use lying but does not need to.

[38] 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.

there is an alignment of interests between the subject and the manipulator, both on the individual and collective levels."[39]

Detailed individualized information in the hands of a firm with interests that diverge from consumers is normally considered dangerous. For example, Roger Allan Ford focuses on malicious actors gaining access to consumer data to scam people. His core argument is that data traffickers help scammers by helping them use hyper-targeting ads to reach the most promising victims, hide from law-enforcement authorities, and develop better and more-effective scams by providing them access to our data.[40] Relatedly, both Kilovaty and Calo analogize to data breach law to recognize "the potential misuse" of breached personal information because the actors holding our data do not have interests that align with consumers. Thus far, scammer and cybersecurity threats are the malicious actors of concern.

But manipulation need not be by overtly malicious actors that seek to break the law. As noted by Lina Khan and David Pozen in their recent article *A Skeptical View of Information Fiduciaries*,[41] technology companies who control user data have interests that diverge from the well-being of their users. In fact, the authors argue (which I do not) that data controllers' interests are seen to be in perpetual conflict with their users.[42] According to Khan and Pozen, data brokers, data traffickers, ad networks, and data controllers all are in a similar situation with interests that are, in the best case, not aligned with consumers and, in the worst case, perpetually divergent from consumers' interests.[43] We need not adopt Khan and Pozen's idea of perpetual conflict

---

[39] Kilovaty, "Legally Cognizable Manipulation," 2019. 466

[40] Roger Allan Ford, "Data Scams," *Hous. L. Rev.* 57 (2019): 111.

[41] Khan and Pozen, "A Skeptical View of Information Fiduciaries."

[42] "Even if we accept for argument's sake the soundness of the predatory/ nonpredatory distinction in this context — although we are doubtful — it is unclear how a digital fiduciary is supposed to fulfill its duty of loyalty to users under conditions of profound and 'perpetual' conflict." Khan and Pozen 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 (XXXX) and Freeman, Wicks, and Parmar for the standard argument against relying on "shareholder wealth maximization" as necessary, useful, or helpful. R Edward Freeman, Andrew C Wicks, and Bidhan Parmar, "Stakeholder Theory and 'the Corporate Objective Revisited,'" *Organization Science* 15, no. 3 (2004): 364–69.

[43] Empirical studies support the idea that data aggregators and hackers have similarly divergent interests from consumers: consumers distrust firms that have been hacked or sell to a data aggregator *to the same degree.* Kirsten Martin, "Breaking the Privacy Paradox," *Business Ethics Quarterly* 30, no. 1 (2020): 65–96. As Ryan Calo aptly suggests, legal intervention would be justified whenever there is a divergence between these interests, leading to one side leveraging this gap in information to her own benefit.

of interests to acknowledge that data traffickers can have interests that diverge from consumers and that there are few market forces to align their interests.[44]

The phenomenon of interest herein focuses on interests diverging between manipulator and target and differs from two alternative definitions of manipulation that focus on (a) the "rationality" of the target's decision or (b) the inappropriateness of the decision. First, a broader approach to manipulation focuses on the degree that the target's decision is deemed "rational," where manipulators are those that circumvent a target's rational decision-making process.[45] Someone is said to have been manipulated if their decision is judged to not be rational *enough*. For example, Sunstein judges a decision to be manipulated "if it does not sufficiently engage or appeal to people's capacity for reflective and deliberate choice."[46]

However, defining manipulation as that which only undermines "rationality" is problematic. First, only a small group of people[47] actually

---

[44] As I have 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 taken into account. Data aggregators are free to collect any information and will pay top dollar for even the lowest quality and with the least privacy expectations respected. Banks 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?," *The Information Society* 32, no. 1 (2016): 51–63.

[45] Spencer, "The Problem of Online Manipulation"; Julia Hanson et al., "Taking Data Out of Context to Hyper-Personalize Ads: Crowdworkers' Privacy Perceptions and Decisions to Disclose Private Information," n.d.; Ido Kilovaty, "Legally Cognizable Manipulation," *Berkeley Tech. LJ* 34 (2019): 449.

[46] Sunstein, "Fifty Shades of Manipulation." 1. For example, Anne Barnill 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, "I'd like to Teach the World to Think: Commercial Advertising and Manipulation." Or engage with intuitive thinking or non-verbal Becher and Feldman, "Manipulating, Fast and Slow: The Law of Non-Verbal Market Manipulations." or even just attempt to influence someone's decision making. (Thaler & Sunstein, 2008, p. 6).). See also Gorin "Do Manipulators Always Threaten Rationality?," *American Philosophical Quarterly* 51, no. 1 (2014): 51–61. and "mentally competent, fully informed individual, through a process of rational self-deliberation" (cites Isaiah berlin Two concepts of liberty). Michal S Gal, "Algorithmic Challenges to Autonomous Choice," *Mich. Tech. L. Rev.* 25 (2018): 59. "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" (Hill, 1991, p. 33). Wilkinson, "Nudging and Manipulation."

[47] Autistic respondents, it turns out, perform the best as "rational" decision makers, leaving

make decisions in a manner that is consistent to what researchers call "rational," thereby leaving the majority of us to continually act in a way that is deemed "irrational" and making the designation do little work in differentiating types of decisions. In other words, all decisions can be seen as not fully rational. Therefore, if all decisions are not sufficiently rational, all decisions are possibly manipulated, making manipulation almost impossible to identify.[48] Because non-rational decisions are ubiquitous, equating manipulation with non-rational decisions allows scholars to declare that manipulation "is everywhere."[49] However, the phenomenon of interest in this article is the tactic to covertly undermine a target's decision towards

non-autistic adults to behave more "irrationally" in their decisions. Mark Brosnan, Marcus Lewton, and Chris Ashwin, "Reasoning on the Autism Spectrum: A Dual Process Theory Account," *Journal of Autism and Developmental Disorders* 46, no. 6 (2016): 2115–25; Benedetto De Martino et al., "Explaining Enhanced Logical Consistency during Decision Making in Autism," *Journal of Neuroscience* 28, no. 42 (2008): 10746–50; George D Farmer, Simon Baron-Cohen, and William J Skylark, "People with Autism Spectrum Conditions Make More Consistent Decisions," *Psychological Science* 28, no. 8 (2017): 1067–76. Rational decisions also remove adaptations that have proven to be evolutionarily desirable such as group survival and altruistic fairness. Nicolas Baumard, Jean-Baptiste André, and Dan Sperber, "A Mutualistic Approach to Morality: The Evolution of Fairness by Partner Choice," *Behavioral and Brain Sciences* 36, no. 1 (2013): 59–78; Sule Guney and Ben Newell, "Fairness Overrides Reputation: The Importance of Fairness Considerations in Altruistic Cooperation," *Frontiers in Human Neuroscience* 7 (2013): 252; Ernst Fehr and Simon Gächter, "Fairness and Retaliation: The Economics of Reciprocity," *Journal of Economic Perspectives* 14, no. 3 (2000): 159–81. The use of "rational" has mistakenly become shorthand for a desirable decisions, however it is no long clear that rational decisions are desirable or that irrational decisions are not desirable.

[48] . One reason "rationality" is put forth as a test for if someone is manipulated is to maintain 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. We do this because we think 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, "Do Manipulators Always Threaten Rationality?" 51.

[49] Shafir, "Manipulated as a Way of Life."

the interests of the manipulator. [50] I do not focus on whether the target's decision making is deemed rational or not.[51]

A narrower alternative definition of manipulation is to require that the end goal of the manipulator is undesirable. For example, Tal Zarsky uses the standard of 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."[52] Similarly, Noggle offers a frequently used definition of manipulation that rests on the intention of the manipulator to move the targets decision in such a way that the manipulator would not even approve of the decision: "manipulation is influence that attempts to get the target to stray from [the influencer's] ideals or rational standards for belief, desire, and emotion." Noggle's version of manipulation "involves influencing in ways the influencers could not themselves accept."[53] Noggle argues that an act is not manipulative if the manipulator (or influencer in this case) "is sincere, that is, in accordance with what the influencer takes to be true, relevant, and appropriate."[54]

This approach places a standard for manipulation that is almost never met; manipulators frequently (and paternalistically) believe their end goal or interests are in the interest of their target. And sometimes manipulators are

---

[50] 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. Becher and Feldman, "Manipulating, Fast and Slow: The Law of Non-Verbal Market Manipulations"; Wilkinson, "Nudging and Manipulation"; Richard H Thaler and Cass R Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Penguin, 2009). Dark patterns. [50] Daniel Susser, "Invisible Influence: Artificial Intelligence and the Ethics of Adaptive Choice Architectures," *Association for the Advancement of Artificial Intelligence (Www.Aaai.Org)*, 2019. Mathur et al., "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites." Choice architectures. Susser, "Invisible Influence: Artificial Intelligence and the Ethics of Adaptive Choice Architectures."

[51] 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, "Digital Market Manipulation."

[52] Zarsky, "Privacy and Manipulation in the Digital Age" 158. For Professor Zarsky, manipulation is based on a standard of rational decisions 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" Zarsky, 168–69.

[53] Christian Coons & Michael Weber, *Manipulation: Investigating the Core Concept and Its Moral Status*, *in* MANIPULATION: THEORY AND PRACTICE 1, 14 (2014).

[54] Robert Noggle, "Manipulative Actions: A Conceptual and Moral Analysis," *American Philosophical Quarterly* 33, no. 1 (1996): 43–55, 50.

acting 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 their disabled patient into taking their medicine. These manipulators are put in a position of caregiving with the expectation that their interests will trump the (poor) preferences of their charge. More importantly, relying on manipulators 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 frequently defend their tactics as in the best interest of consumers.[55]

Manipulation's "wrongness" is not necessarily because the end goal is bad, irrational, or socially undesirable, but because manipulation undermines the target as the author of their own decision and attempts to steer the target's decision towards the manipulator's interests.[56] Manipulation here is agnostic to the decision-making process or interests of the target. The target may be self-interested (or not), a slow deliberator (or not), immune to sensory signals (or not), or online (or not). The manipulator wants to hijack the target's decision towards their own preferences and goals—which diverge from the target's—in a way that covertly leverages the target's weaknesses or vulnerabilities. In fact, it is the divergence of the interests that will make targeted manipulation particularly important for law and economics.

---

[55] According the the Network Advertising Initiative, and industry trade group, targeted advertising "helps keep content free, helps consumers, and empowers the economy." https://www.networkadvertising.org/understanding-online-advertising/ In reaction to a Wall Street Journal article on the how targeted advertising benefits ad network and data traffickers but not consumers or publishers doing the advertising, a chief marketing office claimed "As 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." https://www.forbes.com/sites/daviddoty/2019/08/13/a-reality-check-on-advertising-relevancy-and-personalization/#7765e9397690. The CMO was reacting to a study on who benefits from hyper targeted advertising. Veronica Marotta, Vibhanshu Abhishek, and Alessandro Acquisti, "Online Tracking and Publishers' Revenues: An Empirical Analysis," 2019.

[56]Susser, Roessler, and Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World," 2019. See also Wood, "when getting others to do what you want is morally problematic, that 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." (p.17-18). Wood, "Coercion, Manipulation, Exploitation."

C. Manipulation in Economics

This problematic tactic—the leveraging of individualized knowledge to exploit a target's vulnerabilities in order to covertly undermine their decision making—has been identified as theoretically possible, but unlikely, in two overlapping fields in economics.

First, the economics of advertising examines the costs and benefits of advertising and marketing tactics. 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. Hyper-targeted advertising is framed as efficient so that "advertising is only shown and designed for a select group of consumers who stand to gain most from this information."[57] 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."[58] Better information in the hands of marketers is assumed to benefit the advertisers by being more efficient and to benefit the consumers by only showing ads that interest them.[59] 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.

---

[57] Catherine E Tucker, "The Economics of Advertising and Privacy," *International Journal of Industrial Organization* 30, no. 3 (2012): 326–29, 326. See also Avi Goldfarb and Catherine Tucker, "Digital Economics," *Journal of Economic Literature* 57, no. 1 (2019): 3–43. "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." David S Evans, "The Online Advertising Industry: Economics, Evolution, and Privacy," *Journal of Economic Perspectives* 23, no. 3 (2009): 37–60, 56. See also Tucker, "The Economics of Advertising and Privacy" 326 ("[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.").

[58] Tucker, "The Economics of Advertising and Privacy," 326.

[59] Show that the evidence is mixed in terms of targeted advertising. Goldfarb and Tucker, "Digital Economics.". **While** Goldfarb and Tucker' 2011 article is frequently cited to show that privacy regulations could limit the ability of firms to tailor advertising to a consumer's behavior may reduce online advertising effectiveness, less cited is their more recent work finding that dynamic retargeted ads are on average less effective than their generic equivalent. Tal Z Zarsky, "Online Privacy, Tailoring, and Persuasion," in *Privacy and Technologies of Identity* (Springer, 2006), 209–24.; Goldfarb and Tucker 2013.

However, the economics of advertising, to include product placement and promotion, struggles with incorporating the preferences of the consumer in the analysis when it comes to privacy expectations, trust, and overall unease with advertising or the tracking required.[60] Tucker specifically identifies the issue of the intrusiveness of collection as "consumers may be wary of being tracked too closely by firms and then firms using this information to tailor prices," which was also identified in a similar article by Acquisti and Varian.[61] Scholars studying the economics of information and advertising have identified this problematic tactic—where firms have gained access to intimate consumer information and could 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 studies when firms differentiate prices across customers. Pricing can be based on coupons, group identification, volume of product, etc.[62] Personalized pricing is referred to as

---

[60] Tucker, "The Economics of Advertising and Privacy"; Evans, "The Online Advertising Industry: Economics, Evolution, and Privacy"; Qiaowei Shen and J Miguel Villas-Boas, "Behavior-Based Advertising," *Management Science* 64, no. 5 (2018): 2047–64; Alessandro Acquisti, Curtis Taylor, and Liad Wagman, "The Economics of Privacy," *Journal of Economic Literature* 54, no. 2 (2016): 442–92. As noted by Avi Goldfarb and Catherine 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". Avi Goldfarb and Catherine Tucker "Digital Economics" 22. Consumers may resist having advertising platforms collect detailed information about their browsing behavior Evans, "The Online Advertising Industry: Economics, Evolution, and Privacy."

Seen as a cost, annoyance in sending advertising messages to consumers based on their past purchase behavior Shen and Miguel Villas-Boas, "Behavior-Based Advertising."

And Acknowledged "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, and Wagman, "The Economics of Privacy."

[61] "The Economics of Advertising and Privacy." 326

[62] Curtis R Taylor, "Consumer Privacy and the Market for Customer Information," *RAND Journal of Economics*, 2004, 631–50; Gerhard Wagner and Horst Eidenmuller, "Down by Algorithms: Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions," *U. Chi. L. Rev.* 86 (2019): 581. Third-degree price discrimination is offering different pricing for different groups of people based on observable characteristics—perhaps coupons of versioning Goldfarb and Tucker, "Digital Economics." Second-degree price discrimination is offering different pricing and allowing consumers to choose the pricing that suits them (volume pricing). First degree price discrimination includes personalized pricing. In addition, pricing can include what product is offered at what price to each consumer or group of consumers.

first-degree price discrimination, customized, or targeted pricing, and represents a pricing strategy "whereby firms charge different prices to different consumers based on their willingness to pay."[63] As noted in a symposium for University of Chicago Law Review on the economics of price discrimination, "we are approaching a world in which each consumer will be charged a personalized price for a personalized product or service."[64] For example, Seele et al. uses the classic example of selling Coca-Cola based not on the location or even temperature but based on a consumer's willingness to pay. [65] Given the evolution of marketing online, the current concern is that firms would offer Coca-Cola based on whether someone is a diabetic or addicted to sugar or, perhaps, at a low emotional point. Building on consumer data, pricing algorithms can estimate consumers' willingness to pay or, as Xu and Dukes (2019) state, algorithms gain "superior knowledge" by understanding consumer preferences better than the consumers themselves.

In one of the first examinations of personalized pricing, Acquisti and Varian analyzed conditioning prices on consumer purchase history. [66] At the time, the personalized pricing analysis assumed consumers (a) knew the firms conducting the price discrimination and (b) were emboldened to take their business elsewhere if the price discrimination was unwanted. At the time, it was assumed that the price discrimination would make the pricing more accurate and efficient and, therefore, beneficial to the consumer (or they would leave the transaction).[67]

---

[63] Vidyanand Choudhary et al., "Personalized Pricing and Quality Differentiation," *Management Science* 51, no. 7 (2005): 1120–30. P. 1120. See also Paul Heidhues and Botond Kőszegi, "Naivete-Based Discrimination," *The Quarterly Journal of Economics* 132, no. 2 (2017): 1019–54; Alessandro Acquisti and Hal R Varian, "Conditioning Prices on Purchase History," *Marketing Science* 24, no. 3 (2005): 367–81; Hal Varian, "Artificial Intelligence, Economics, and Industrial Organization" (National Bureau of Economic Research, 2018).

[64] Bar-Gill, "Algorithmic Price Discrimination When Demand Is a Function of Both Preferences and (Mis) Perceptions" 86 U. Chi. L. Rev. 217, 217. 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. Varian Varian, "Artificial Intelligence, Economics, and Industrial Organization." finds personalized pricing unrealistic.

[65] Peter Seele et al., "Mapping the Ethicality of Algorithmic Pricing: A Review of Dynamic and Personalized Pricing," *Journal of Business Ethics*, 2019, 1–23.

[66] "Conditioning Prices on Purchase History."

[67] E.g., assume "Thus, 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." Acquisti and Varian 368.

However, these assumptions no longer hold given current abilities in marketing online. First, firms seeking to price discriminate are unknown by the 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 our parlance). Seele et al., in their analysis of price discrimination, 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 personal characteristics such as location data, browsing and purchasing history, social media posts and 'likes,' and so on."[68]

Second, consumers cannot be considered emboldened.[69] As noted more recently by Acquisti et al., "[p]ersonal 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 themselves do not have access to those markets: they cannot yet efficiently buy back their data, or offer their data for sale."[70] 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 of manufacturing preferences and artificially shifting consumption patterns.[71] When price discrimination "targets misperceptions, specifically demand-inflating misperceptions," then price discrimination may hurt consumers and may reduce efficiency.[72] The

---

[68] Peter Seele et al., "Mapping the Ethicality of Algorithmic Pricing: A Review of Dynamic and Personalized Pricing," *Journal of Business Ethics*, 2019, 9.

[69] 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, as happened after the famous Amazon.com price experiment (Streifeld 2000). Acquisti and Varian, "Conditioning Prices on Purchase History." (p. 367-368)

[70] "The Economics of Privacy." 447

[71] Wagner and Eidenmuller, "Down by Algorithms: Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions." "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 and Eidenmuller 602.

[72] 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, "Algorithmic Price Discrimination When Demand Is a Function of Both

economics of price discrimination has (until recently) been able to hold constant consumer preferences or assume that hyper-targeting and personalized pricing is beneficial, therefore making the type of targeted consumer manipulation that is the subject of this paper not a concern.[73]

In sum, both the economics of advertising and the economics of price discrimination have identified the often assumed-away scenario of the use of intimate knowledge to covertly manipulate a consumer through advertising, product placement, or pricing. Wagner and Eidenmuller nicely summarize this 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."[74] The possibility of a firm gaining a position of power to manipulate consumers—with the intimate knowledge of the consumer as well as the reach to target their decision making covertly—has always been a possibility in economics but considered highly unlikely with empowered and knowledgeable consumers. More recent work in economics has begun to grapple with the reality we face where firms are now in the position to manipulate millions of consumers online without any governance or safeguards in place.

Preferences and (Mis) Perceptions." 217

[73] Justin P. Johnson notes that the cost of losing trust of consumers is not included at all in the calculation to use manipulative tactics in marketing such as psychometric profiling and hyper-targeted advertising. Justin P Johnson, "Targeted Advertising and Advertising Avoidance," *The RAND Journal of Economics* 44, no. 1 (2013): 128–44. Florian Hoffmann, Roman Inderst, and Marco Ottaviani provide a good 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 make individual or collective decisions, whether Örms are able to personalize prices, and whether receivers are wary of the sendersíincentives to become better informed." Florian Hoffmann, Roman Inderst, and Marco Ottaviani, "Persuasion through Selective Disclosure: Implications for Marketing, Campaigning, and Privacy Regulation," *Management Science*, 2020.

[74] Wagner and Eidenmuller, "Down by Algorithms: Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions." 607

III. MANIPULATION AND CONSUMER CHOICE

Online firms are now in the position to manipulate consumers with data about individuals' weaknesses as well as the reach to covertly influence a target's decisions. We have a scenario predicted as possible, worrisome by economists but unlikely due to presumed structural and market barriers. Economists 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. In other words, the base assumption was that consumers would always be enabled to prevent their information from falling into the hands of firms capable of manipulating them. This is normally a very reasonable assumption. Offline market actors do not disclose information about preferences, concerns, forecasts, etc. without safeguards in place to protect against possible manipulation.

Importantly, firms are in the position to manipulate thereby undermining an individual's ability to enact their preferences through choice. A defining feature of the 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.

I next turn to examine the danger of targeted manipulation in undermining consumer choice in the market. We generally seek 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[75] 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.[76] In fact, as I explore here, authentic consent is critical to markets and economics. I position targeted online manipulation—the covert leveraging of vulnerabilities to

---

[75] Susser, Roessler, and Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World," 2019.

[76] Friedrich August Hayek, "The Use of Knowledge in Society," *The American Economic Review* 35, no. 4 (1945): 519–30; Ronald Harry Coase, "Problem of Social Cost, The," *Journal of Law and Economics* 3 (1960): 1; Zarsky, "Privacy and Manipulation in the Digital Age."

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, 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" or "voluntary private bargaining" are used to explain market actors and transactions.[77] In deciding to transact, individuals search and gather information as to the terms, bargain over those terms, and make a decision based on their knowledge of their preferences, needs, and information on the ground.[78] That choice is the enactment of preferences, or as close as we can get. We protect the voluntary character of an exchange and seek to identify actions that could undermine choice-as-consent (Sandel).[79]

Choice-as-consent is the air that the modern economist breathes. "[B]y choosing, individuals reveal that they agree with or consent to the conditions under which the choice was made." [80] The argument behind the exaltations of choice-as-consent is that each individual is best able to identify weigh, argue, enact in their best interest. When choosing a mortgage lender, I am able to determine which factors – timelines, rate, responsiveness – are

---

[77] 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" See Friedman (1962, p. 14), And Martin in JBE. "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" Hayek, "The Use of Knowledge in Society" 524. **See also** GORDON R FOXAL, THE BEHAVIOR ANALYSIS OF CONSUMER CHOICE 581-582 (2003). Coase defends choice as better than any interference. Coase, "Problem of Social Cost, The." 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," *Journal of Political Economy* 58, no. 4 (1950): 328–46..

[78] Coase, "Problem of Social Cost, The."

[79] See Buchanan, James M., and Gordon Tullock. *The calculus of consent*. Vol. 3. Ann Arbor: University of Michigan Press, 1962.

[80] Alain Marciano, "Freedom, Choice and Consent. A Note on a Libertarian Paternalist Dilemma," *Homo Oeconomicus* 32, no. 2 (2015): 287–91, 288.

important to me; my choice reflects my preferences. Choice-as-consent is critical to allow individuals to retain autonomy and choose since "individuals know better than anyone else what is best for them."[81]

In undermining an individual's choice in the market, manipulation is a close cousin to coercion and fraud. Raz links manipulation to coercion where both "subject the will of one person to that of another," which violates their independence and is inconsistent with their autonomy.[82] 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.[83] Where the target must know about coercion for it to work, manipulation only works if hidden from the target. The manipulator would have us believe that we make up our own minds by distorting the reality of our situation.[84] Table 1 summarizes how manipulation, fraud, and coercion work to undermine consumer choice and how targeted manipulation is closer to coercion and fraud rather than persuasion as a tactic to "influence" decision making.

Table 1

	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

[81] Gal, "Algorithmic Challenges to Autonomous Choice" 76. In doing so, individuals are able to choose based on their preferences as formed within their lived experience.

[82] Raz, *The Morality of Freedom*, 387. Raz states that autonomy as part of a social ideal and is opposed to a life of coerced choices. Raz, *The Morality of Freedom*, 378.

[83] Raz, *The Morality of Freedom*; Wilkinson, "Nudging and Manipulation." 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, 345. For Raz, manipulation 'perverts the way [a] person reaches decisions, forms preferences or adopts goals'.[20]20 Raz, ibid 377–78.

[84] Konstantinos Kalliris, "Self-Authorship, Well-Being and Paternalism," *Jurisprudence* 8, no. 1 (2017): 23–51.

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."[85] For Wilkinson, manipulation "is intentionally and successfully influencing someone using methods that pervert choice."[86]

B. Why We Protect Choice

Manipulation is in a family of tactics that undermines consumer choice in the market, tactics which are the subject of regulations and safeguards.[87] We protect choice for three reasons: autonomy of the individual, efficiency of individual transactions, and 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."[88] Autonomy is critical to individuals to "have unique access to their situations, their constraints, and their tastes."[89] This drive for autonomy is a drive for liberty and provides a grounding for our political, social, and economic lives.[90] As noted by Isiah 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,

---

[85] Posner, "The Law, Economics, and Psychology of Manipulation."

[86] Wilkinson, "Nudging and Manipulation" 347.

[87] Tactics that include fraud, coercion, misrepresentation, undue influence, etc. These are covered in a later section.

[88] 13 Raz, *The Morality of Freedom* (n 5) 369

[89] Sunstein, "Fifty Shades of Manipulation" 228.

[90] Burkell and Regan, "Voter Preferences, Voter Manipulation, Voter Analytics: Policy Options for Less Surveillance and More Autonomy"; Amartya Sen, "Liberty and Social Choice," *The Journal of Philosophy* 80, no. 1 (1983): 5–28; Amartya Sen, "Individual Preference as the Basis of Social Choice," in *Social Choice Re-Examined* (Springer, 1997), 15–37.

> not being decided for . . . .[91]

Autonomy is an end worth protecting not in terms of optimizing a decision or in service of some larger good but because maintaining autonomy allows an individual to be the author of her own decisions.[92] Someone who is autonomous is able to evaluate options, assess plans, and decide what is best.[93] Kalliris summarizes, "Coercion and manipulation undermine autonomy because they interfere with this decision-making process."[94] If individuals are manipulated, "they are deprived of the (full) ability to make choices on their own simply because they are not give a fair or adequate chance to weigh all variables."[95] Manipulation disrupts a target's capacity for self-authorship by allowing another person to decide how and why they ought to live.[96] Manipulation's challenge to individual autonomy as self-authorship is "its deeper, more insidious harm."[97]

2. Efficiency

Efficiency is the ultimate rationale for authentic choice for economists and is why economic theory relies on choice.[98] Not allowing consumers to make their own choice based on their preferences and in pursuit of their interests is seen to be inefficient and leads to suboptimal transactions.[99] The individual

---

[91] Isaiah Berlin "Two Concepts of Liberty,"

[92] Susser, Roessler, and Nissenbaum, "Technology, Autonomy, and Manipulation."

[93] Kalliris, "Self-Authorship, Well-Being and Paternalism" 8.

[94] Kalliris.

[95] Sunstein, "Fifty Shades of Manipulation" 228.

[96] "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" Susser, Roessler, and Nissenbaum, "Technology, Autonomy, and Manipulation" 8. Manipulation "subverts and insults a person's autonomous decision making" Wilkinson, "Nudging and Manipulation" 345.

[97] Susser, Roessler, and Nissenbaum, "Technology, Autonomy, and Manipulation" 1. See also Kalliris, "Self-Authorship, Well-Being and Paternalism."

[98] Authentic choice is free from manipulation, coercion, fraud, deception, etc – or as close as we can get.

[99] Zarsky, "Privacy and Manipulation in the Digital Age"; Calo, "Digital Market Manipulation." "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 172. "consumers confronted with manipulation

"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."[100] The individual knows their own tastes, values, interests, and preferences. For example, I know what I need in a lender, doctor, or university. As 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 in that 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.[101]

Individuals are in the position to understand their competing demands and preferences and to make the best decision in their interest.[102]

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 make a decision based on their values, interests, and preferences. Fabienne Peter

---

eventually do not act in accordance with their preferences, thus leading to suboptimal outcome" Zarsky, "Privacy and Manipulation in the Digital Age" 173.

[100] Mill On Liberty p. 14. See also In DeGregorio and Ranchordas Giovanni De Gregorio and Sofia Ranchordas, "Breaking Down Information Silos with Big Data: A Legal Analysis of Data Sharing," *New Legal Challenges of Big Data (Edward Elgar, 2020, Forthcoming)*, 2019.. Book quotes Mill On Liberty. "The only purpose for which power can be rightfully exercised over any member of a civilized 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." Mill 17. Mill is often cited to explain why society supports choice-as-consent at the level of the individual (Susser, Posner, Gal).

[101] Hayek, "The Use of Knowledge in Society," 521–22.

[102] Jacob Viner, in his use of Bentham to explain the role of choice, notes "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." Viner, "The Intellectual History of Laissez Faire" 65.

summarizes, **"**The emphasis in economic theory on freedom of choice in the market sphere suggests that legitimization in the market sphere is 'automatic' and that markets thus avoid the typical legitimization problem of the state."[103] Freedom of choice for Peters, is the foundation of efficient and autonomous decisions that allows us to declare the market to be legitimate.

Manipulation, in undermining consumer choice, leads to the transactional sins of diminishing the autonomy of the decision maker and inefficiently allocating resources. These transaction sins aggregate to diminish the legitimacy of the market. In other words, choice-as-consent helps justify the moral legitimacy of transactions as a whole.[104] Markets are legitimate because each transaction was voluntary and free, without coercion, fraud, deception, or manipulation.[105]

C. How We Protect Authentic Choice in the Market

Manipulation is hardly the only problematic behavior that seeks to undermine authentic choice. To preserve market integrity and legitimacy, we protect choice in the market by seeking to eradicate any interference with private preferences.[106] For example, we protect choice by protecting market actors negotiating under duress, and seek to prevent contractors from acting in bad faith,[107] opportunistically, or unconscionably.[108] We also aggressively govern deception in the law,[109] including false suggestions, concealment of

---

[103] (Peters 2004, p. 1). Peter, Fabienne, "Choice, Consent, and the Legitimacy of Market transactions".

[104] Robin West, "Authority, Autonomy, and Choice: The Role of Consent in the Moral and Political Visions of Franz Kafka and Richard Posner," *Harvard Law Review*, 1985, 384–428.

[105] Robert Nozick, *Anarchy, State, and Utopia*, vol. 5038 (New York: Basic Books, 1974). E.g., When the SEC investigates and prosecutes insider trading and fraud, they do so in pursuit of maintaining legitimacy of the market.

[106] Sunstein 1986

[107] In every contract is the implied duty of good faith and fair dealing in the performance and enforcement of the contract. The implied duty of good faith helps to protect consumers by ensuring that parties with whom the consumer contracts acts honestly and does not take advantage of the consumer in the performance of their contract. Restatement (Second) of Contracts § 201 (AM. LAW INST. 1981). U.C.C. § 1-304 (AM. LAW. INST. & UNIF. LAW. COMM'N 2017). 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 (AM. LAW. INST. & UNIF. LAW. COMM'N 2017).

[108] Posner, "The Law, Economics, and Psychology of Manipulation."

[109] Lying, misleading, and falsely denying: how moral concepts inform the law of

truth, deception about facts, opinions, or law and even intentional ambiguities.[110]

We can also see the protection of authentic choice as consent in the work on vulnerable consumers. Vulnerable consumers are those actors in the market who are seen as limited in their ability to authentically consent to a transaction.[111] Vulnerability is not necessarily a permanent attribute of a relationship or an individual, and consumers can move in and out of contexts making them vulnerable.[112] Individuals are considered vulnerable when at key life stages[113] or when battling health challenges[114] or when in a temporarily vulnerable position, such as after a hurricane or natural disaster.

In sum, tactics that undermine choice-as-consent, such as misrepresentation, power imbalances, coercion, and fraud, are problematic because consumer choice under these conditions is not seen as an authentic or actual operationalization of their preferences. Until now, choice has been actively protected in markets in order to preserve individual autonomy, transaction efficiency, and market legitimacy.

D. How We Normally Regulate Manipulation

Manipulation is regulated offline. Normally, the power to manipulate comes within 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.

---

perjury, fraud, and false statements" Stuart Green

[110] Larry Alexander and Emily Sherwin, "Deception in Morality and Law," *Law and Philosophy* 22, no. 5 (2003): 393–450.

[111] 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," *The Dark Side of CRM: Customers, Relationships and Management*, 2015, 122.

[112] Batt Book

[113] E.g., puberty, peer rejection, low socioeconomic status, family disharmony, (all Nairn),

[114] or Marlys Mason and Teresa Pavia – health challenges impact the agency and identity of the consumer (examine late stage AIDS, breast cancer patients, chronic illness, parents of significant disability).

Normally, sharing information with a particular market actor, a firm or individual, requires trust and other safeguards such as professional duties, contracts, negotiated alliances, nondisclosure agreements, etc. A supplier might craft a contract, NDA, or even enter into an alliance in order to safely share their concerns, preferences, forecasts, and risks. For individuals, we similarly share such information in trusted relationships, such as with our lawyers, therapists, or advisors. Individuals do not share details with a car salesperson, such as how poorly their current car is running or changes in their household finances, because the car salesperson would then use that information against the individuals and not in their interest.[115] Offline, manipulation is prevented by ensuring market actors with intimate information about vulnerabilities are prevented from using that information against the target.[116]

[115] As noted in his article in the *Journal of Economic Perspectives, "*People with private information may not readily reveal it, especially if they know that it will be used in a decision that affects them." Joseph Farrell, "Information and the Coase Theorem," *Journal of Economic Perspectives* 1, no. 2 (1987): 113–29, 117.

[116] Professor Ryan Calo refers to this as economic intimacy in a larger argument that discriminately sharing information between market actors is good for markets. Ryan Calo, "Privacy and Markets: A Love Story," *Notre Dame L. Rev.* 91 (2015): 649. In business, we focus on a Coasian analysis of the safeguards required to share information – with sharing information considered both risky and rewarding for markets and market actors Jeffrey S Harrison, Douglas A Bosse, and Robert A Phillips, "Managing for Stakeholders, Stakeholder Utility Functions, and Competitive Advantage," *Strategic Management Journal* 31, no. 1 (2010): 58–74. Kirsten Martin and Robert Phillips. Stakeholder Friction. 2020.

IV. ORIGINAL MARKET SIN: PRIVACY-AS-CONCEALMENT

This situation is odd: where firms are able to collect and covertly use individualized information to undermine consumer decisions. The incarnation of targeted manipulation online divorces the intimate knowledge of the target and the reach used to manipulate from a specific relationship. Online, we now have a situation where firms, with whom we have no relationship, have more information about our preferences, concerns, and vulnerabilities than doctors, lawyers, or therapists. In addition, these firms have an ability to reach specific targets due to the hyper-targeting mechanisms available online. Yet, we are not privy to who has access to that information when a company approaches us with targeted product suggestions or advertising.[117]

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, I turn to examine 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 Helen Nissenbaum notes, "anything goes," relies on privacy as only that which is concealed. In disclosing, individuals are mistakenly framed as relinquishing any expectations of privacy and the information is no longer governed by formal or informal norms.[118]

After connecting the original sin of the market as defining privacy-as-concealment, where disclosed information no longer has privacy expectations, to consumer manipulation, I will then illustrate the influence of

---

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

[118] Now in the U.S we are at the point where individuals do not need to even 'disclose' information. In just being, individuals are assumed to be tracked.

privacy-as-concealment in how we study and regulate privacy in economics and policy.

A. Privacy-as-Concealment

In an important examination of the economics of privacy, Acquisti et al. link privacy-as-concealment to work 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,"[119] where consumer privacy is equated to consumer ability to conceal information.[120] This definition was useful to the field since privacy-as-concealment is easy to identify and model in economic analysis; market actors would make a binary (and easily measured) decision to either conceal information (protect privacy) or disclose it (relinquish privacy). [121]

---

[119] "What Is Privacy Worth?," *The Journal of Legal Studies* 42, no. 2 (2013): 249–74, 251. See also Avi Goldfarb, "What Is Different about Online Advertising?," *Review of Industrial Organization* 44, no. 2 (2014): 115–29. Both Posner and Stigler frame the concealment as information as "private" and the disclosure of information as not private. Richard A Posner, "The Economics of Privacy," *The American Economic Review* 71, no. 2 (1981): 405–9; Richard A Posner, "The Right of Privacy'(1978)," *Georgia Law Review* 12 (n.d.): 393; George J Stigler, "An Introduction to Privacy in Economics and Politics," *The Journal of Legal Studies* 9, no. 4 (1980): 623–44.

[120] Stigler and Posner also posit privacy (as concealment) as either increasing or diminishing the "wealth of society" and 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." Cohen, "Privacy, Ideology, and Technology: A Response to Jeffrey Rosen" 232. I agree with this second critique of the foundations of the economics of privacy. Here I focus on the fallacy that privacy is only that which is concealed.

[121] Contrary to popular musings about privacy having no definitions, privacy definitions fall into three categories broadly; 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 where information that is concealed is private. This definition is attractive for practical reasons in that it is easy to measure (someone discloses information or does not) in surveys and in the field. Further, it 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 is further explored below. See Professor Daniel Solove and the anthology editied by Professor

This approach to defining privacy renders privacy as inefficient to a functioning market since (in principle) relevant information could be helpful to better transactions.[122] Privacy-as-concealment fed easily into the economics of information scholarship which focused on information as critical for markets to run efficiently, including marriage markets, consumer goods markets, and employment markets.[123] Economists could then summarize: "privacy is harmful to efficiency because it stops information flows that would otherwise lead to improved levels of economic exchange."[124] Since information is, in general, important to reducing transaction costs, such as the ability to identify and find trading partners, settle on a price, close the transaction, less information is broadly framed as bad or inefficient for the market.[125]

More importantly, privacy-as-concealment is the tool that has allowed firms to gather and use intimate information about consumers that is then used to covertly undermine their decisions. Privacy-as-concealment is important to understand the current economic anomaly where firms with interests not aligned with consumers have intimate information about individuals. For privacy-as-concealment, disclosed information is not governed by privacy expectations since the information is no longer concealed. In disclosing information, or merely being in public or being

---

Schoemann for overviews of the definition of privacy. Ferdinand David Schoeman, *Philosophical Dimensions of Privacy: An Anthology* (Cambridge University Press, 1984); Daniel J Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, 2006, 477–564.

[122] Stigler, "An Introduction to Privacy in Economics and Politics."

[123] Posner, "The Economics of Privacy"; Stigler, "An Introduction to Privacy in Economics and Politics" 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.")

[124] Benjamin E Hermalin and Michael L Katz, "Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy," *Quantitative Marketing and Economics* 4, no. 3 (2006): 209–39, 211. Traditionally, concealment is considered inefficient: "it 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."p. 406. However, Hermalin and Katz find "(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."

[125] The theory in economics based on privacy-as-concealment 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.

online, consumers are seen as relinquishing privacy. Firms are then permitted, or even expected, to gather, aggregate, sell, and use the information to create value for themselves.

However, privacy-as-concealment was put forward under very specific assumptions by Posner and Stigler. Their arguments assumed that information would only be shared if consumers trusted the other party and that information sharing would always be helpful to the consumer. Specifically, Posner and Stigler assumed the following:

(a) Firms will never gather too much information. The cost will dissuade firms from "idly" surveilling people.[126]

(b) Data gathering, storage, and retrieval was assumed to be expensive and time consuming that no company would store, sell, and traffic in data. Firms would always ask for information directly from the consumer.[127]

(b) Extraneous information will be ignored.[128]

(c) If the collection, sharing, and use of data violated expectations or norms, the cost of upsetting individuals would be felt by those actually

---

[126] Posner, "The Right of Privacy'(1978)." Stigler, "An Introduction to Privacy in Economics and Politics"; Posner, "The Right of Privacy'(1978)." "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

[127] ." Stigler, "An Introduction to Privacy in Economics and Politics" 628. "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." P. 625 Stigler, "An Introduction to Privacy in Economics and Politics.".

[128] Inappropriate information will not be used in decisions (race/sex): "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." Stigler, "An Introduction to Privacy in Economics and Politics" 625. 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." Posner, "The Economics of Privacy."

gathering and storing the data.[129] Therefore, all collection, sharing, and use of information would be sanctioned by the empowered consumer.

The assumption was that the market would fix bad behavior in regards to data collection and use; if an organization collected intrusive information or collected information in a coercive manner, people would walk and the company would have lower quality employees or no customers. Plus, the economists assumed people would not reveal their information, especially if they knew that it would be used in a decision that affects them.[130] Therefore, at the time, the economists could assume that the interests between the individual and the firm were aligned (better advertising, better product offerings, better transaction costs, etc.).

These assumptions may have worked during the first wave of privacy scholarship in economics, when the only actor who had the money and reach to collect large amounts of information was the government.[131] However, the proliferation of data trackers and the ease, value, and cost of trafficking information render these assumptions almost quaint. Storage, retrieval, and sharing are cheap and accurate, and data traffickers collecting and using data have no relationship with the consumer. In fact, these facets of the information economy—cheap and easy collection and storage of data and an ability to make sense of the data to target individuals—are lauded as important steps forward in the advancement of AI and Big Data. However, these same facets of the information economy also undermine the key

---

[129] The requesting organization—government or private actor—will feel the market effects of requesting inappropriate information. "[I]t will pay for this burden through higher wage rates or lower quality employees." Stigler, "An Introduction to Privacy in Economics and Politics" 627. If it is the state doing it, we can assume they are correct in asking for it. Stigler..

[130] Farrell, "Information and the Coase Theorem."

[131] The first assumption in this era of scholarship was that the entity that could surveil consumers was the government as they were the only actors with the money and reach to collect data: **"**Governments (at all levels) are collecting information of a quantity and in a personal detail unknown history. Consider: it would have been quite impossible for a public official in 1860 to learn anything of 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 answer the question, to say nothing of the fact that perhaps one family or four receives payments directly or indirectly from the federal government." (p. 623, Stigler "An Introduction to Privacy in Economics and Politics")

assumptions made in putting forth privacy-as-concealment as useful or reflective of privacy expectations.[132]

B. Reach of Privacy-as-Concealment

Yet, privacy-as-concealment infects our academic and public policy discourse, and the Stigler/Posner approach provided the building blocks of regulatory and academic examinations of privacy.[133] Privacy-as-concealment has remained a force in marketing, economics, public policy, and law; privacy-as-concealment guides the generalizations made about surveys and the implications drawn 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 they would be willing to accept (WTA) a privacy violation. WTA/WTP scholarship relies on privacy-as-concealment by measuring the respondents' willingness to pay to conceal information and equating that with privacy.[134] This research broadly measures consumers' valuation of "privacy" by measuring a valuation of concealment, thereby not allowing information to be disclosed within privacy expectations.[135] Similar measurements of privacy concerns operationalize

---

[132] From Varian (2018): Tucker (2018) also emphasizes that privacy in its current, 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*, 2015, 201.

[133] Goldfarb, "What Is Different about Online Advertising?"; Acquisti, Taylor, and Wagman, "The Economics of Privacy."

[134] "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."Acquisti, John, and Loewenstein, "What Is Privacy Worth?" 249.

[135] Angela G Winegar and Cass R Sunstein, "How Much Is Data Privacy Worth? A Preliminary Investigation," *Journal of Consumer Policy* 42, no. 3 (2019): 425–40; or "We 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 incentivecompatible mechanism to capture individuals' willingness-to-accept (WTA) for a privacy disclosure in a series of three randomized experiments." p. 375 Joseph R Buckman, Jesse C Bockstedt, and Matthew J Hashim, "Relative Privacy Valuations under Varying Disclosure Characteristics," *Information Systems Research* 30, no. 2 (2019): 375–88.

privacy as whether consumers reveal their income in a survey.[136] This leads academics to generalize every disclosure of information as an indication that consumers or respondents do not value privacy.

The 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 surveys and their actual behavior. For example, respondents would indicate a concern for privacy in a survey and then researchers would measure whether the respondents would disclose information online or to researchers or report to have used a social networking app.[137] Researchers would then generalize the study to posit that people claim to care about privacy but show little concern about it in their daily behavior.[138]

Importantly, the evidence of individuals not caring about privacy, or relinquishing privacy in practice, centers on merely disclosing information. For example, 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 they do not care about privacy: "Thirty percent 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."[139] Similarly, in a

---

[136] "[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 and Catherine Tucker, "Shifts in Privacy Concerns," *The American Economic Review* 102, no. 3 (2012): 349–53, 349.

[137] Norberg et al., in one of the first articles naming the privacy paradox, explicitly defines privacy to that which is concealed where the paradox lies in the inconsistency between respondent's intentions to disclose and their actual disclosure behavior. Patricia A Norberg, Daniel R Horne, and David A Horne, "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs* 41, no. 1 (2007): 100–126.

[138] Professors Acquisti, Brandimarte, and Loewenstein summarize the definition and operationalization of the privacy paradox. Alessandro Acquisti, Laura Brandimarte, and George Loewenstein, "Privacy and Human Behavior in the Age of Information," *Science* 347, no. 6221 (2015): 509–14.

[139] Nina Gerber, Paul Gerber, and Melanie Volkamer, "Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior," *Computers & Security* 77 (2018): 226–61, 227. Gerber et al. provide a literature review of the many ways individuals have shown to act paradoxically and summarize, "On 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

summary of information privacy scholarship, Smith et al. note 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."[140] The proof of (not) caring about privacy in practice is demonstrated, according to privacy paradox researchers, by consumers (not) concealing information.

To explain the penchant to disclose information, scholars have linked the paradoxical behavior to the privacy calculus.[141] Individuals relinquish information (framed by scholars as relinquishing privacy[142]) 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 concealed is considered private.[143]

I say the privacy paradox is the most dangerous concept emanating from the privacy-as-concealment framing because research perpetuating the privacy paradox encourages firms to increase the collection and use of personal information without needing to worry about privacy expectations. Consumer-facing firms, marketers, and advertising advocacy groups use the

---

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." Nina Gerber, Paul Gerber, and Melanie Volkamer, "Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior," *Computers & Security* 77 (2018): 226–61, 227.

[140] H Jeff Smith, Tamara Dinev, and Heng Xu, "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* 35, no. 4 (2011): 989–1016, 993.

[141] As I explain, for the privacy paradox to persist as possible, one of two assumptions is necessary: (a) that when consumers disclose information and engage with firms, they also relinquish privacy expectations (there is no privacy), or (b) that privacy is a preference that is easily negotiated away in the market (the so called privacy calculus argument where privacy is easily purchased). Philosophers and law 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. Martin, "Breaking the Privacy Paradox."

[142] Gerber, Gerber, and Volkamer, "Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior"; Paul A Pavlou, "State of the Information Privacy Literature: Where Are We Now and Where Should We Go?," *MIS Quarterly*, 2011, 977–88.

[143] Researchers equate the disclosure of information to "privacy-compromising behavior" in validating the privacy paradox. Susanne Barth and Menno DT de Jong, "The Privacy Paradox–Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior–A Systematic Literature Review," *Telematics and Informatics* 34, no. 7 (2017): 1038–58, 1039.

privacy paradox to justify their current data practices, while also reporting data that shows that consumers overwhelmingly find such practices problematic and creepy.[144] Framing individuals as acting "paradoxically" when disclosing information or going online or using an app in regards to privacy relies upon a definition of privacy as only that which is concealed.[145]

C. Alternative Approaches to Privacy

Defining privacy as that which is concealed has infected economics, public policy, social science and legal scholarship, thereby leading scholars and practitioners to argue that individuals have relinquished privacy expectations when information is disclosed. However, scholarship has begun to theorize as to the privacy of revealed or public information.[146] This shift is critical for this article, since these theories—that disclosed information retains privacy expectations—would not allow intimate knowledge of individuals' vulnerabilities in the hands of firms who can manipulate targets.

Rather than see the disclosure of information as a signal of relinquishing privacy, more context dependent definitions of privacy posit the individual

---

[144] Martin, "Breaking the Privacy Paradox"; Spyros Kokolakis, "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon," *Computers & Security* 64 (2017): 122–34.

[145] In fact, the term 'paradox' is defined as "seemingly absurd or self-contradicting statement or proposition that, *when investigated or explained*, may prove to be well founded or true." *Merriam-Webster Dictionary,* online, s.v. "paradox," italics added. https://www.merriam-webster.com/dictionary/paradox. I thank Alessandro Acquisti for pointing out the actual definition of paradox in reference to the privacy paradox. Many have gone on to investigate the 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. Waldman, "Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'"; Acquisti, Brandimarte, and Loewenstein, "Privacy and Human Behavior in the Age of Information." In fact, contrary to the privacy paradox, consumers retain strong privacy expectations even after disclosing information. Martin, "Breaking the Privacy Paradox." Referring to going online or using an app as somehow paradoxical in regards to privacy would be like calling 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.

[146] A few who specifically address the idea of privacy in public include, Helen Nissenbaum, "Protecting Privacy in an Information Age: The Problem of Privacy in Public," *Law and Philosophy* 17, no. 5 (1998): 559–96; Robert Gellman, "Public Records—Access, Privacy, and Public Policy: A Discussion Paper," *Government Information Quarterly* 12, no. 4 (1995): 391–426; Woodrow Hartzog, "The Public Information Fallacy," 2017; Joel R Reidenberg, "Privacy in Public," *University of Miami Law Review* 69 (2014): 141.

sharing information within a specific community or relationship of trust, or within a specific context of privacy norms.[147] Professor Ari Waldman offers a theory of privacy, privacy as trust, as counter to the "traditional division between public and private." For privacy as trust, individuals disclose information within trust relationships -- with expectations as to how the information will be shared and used.[148] Relatedly, Professors Woody Hartzog and Neil Richards position privacy as reinforcing trust within established relationships.[149] Separately, Professor Hartzog suggests that information disclosed carries with it an understanding of confidentiality—as to how that information should be used and shared—that should carry forward to all other parties who are given access to that information.[150] Each approach 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, others have sought to identify specific types of disclosed information—sensitive,[151] sexual,[152]

---

[147] The list of scholars carving out the privacy norms around disclosed information is long. Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, 2010); Helen Nissenbaum, "A Contextual Approach to Privacy Online," *Daedalus* 140, no. 4 (2011): 32–48; Ari Ezra Waldman, "Privacy as Trust: Sharing Personal Information in a Networked World," *U. Miami L. Rev.* 69 (2014): 559; Richards and Hartzog, "Taking Trust Seriously in Privacy Law"; Danielle Keats Citron, "Cyber Civil Rights," *BUL Rev.* 89 (2009): 61; Kirsten Martin, "Understanding Privacy Online: Development of a Social Contract Approach to Privacy," *Journal of Business Ethics* 137, no. 3 (2016): 551–69, https://doi.org/10.1007/s10551-015-2565-9; Woodrow Hartzog, "Chain-Link Confidentiality," *Ga. L. Rev.* 46 (2011): 657; Daniel J Solove, "'I've Got Nothing to Hide'and Other Misunderstandings of Privacy," *San Diego Law Review* 44 (2007): 745. Or measuring privacy norms in public Joseph Turow et al., "Americans Reject Tailored Advertising and Three Activities That Enable It," *Available at SSRN 1478214*, 2009; Pew Research Center, "Public Perceptions of Privacy and Security in the Post-Snowden Era," 2014, http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

[148] "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." Waldman, "Privacy as Trust: Sharing Personal Information in a Networked World" 559.

[149] "[P]rivacy can and should be thought of as enabling trust in our essential information relationships" Richards and Hartzog, "Taking Trust Seriously in Privacy Law" 431.

[150] A chain-link confidentiality regime would contractually link the disclosure of personal information to obligations to protect that information as it is disclose downstream". P. 659. Hartzog, "Chain-Link Confidentiality."

[151] Ohm, "Sensitive Information."

[152] "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);

intellectual,[153] or sheer quantity[154]—as requiring privacy protection post disclosure. Professor Julie Cohen argues, 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.[155] 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.[156]

Previously, I have argued for a social contract approach to privacy wherein individuals discriminately share information within a community with an understanding of the privacy norms governing that community. Individuals reveal information understanding who would be able to receive that information as well as how and why the information would be used.[157] When we talk about privacy expectations, we are identifying the implicit and explicit norms about how information is expected to flow in a given community.[158]

---

their sexual desires, fantasies, and thoughts; communications related to their sex, sexuality, and gender; and intimate activities (including, but not limited, to sexual intercourse)." Danielle Keats Citron, "Sexual Privacy," *Yale LJ* 128 (2018): 1870, 1880.

[153] "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." Neil M Richards, "Intellectual Privacy," *Texas Law Review* 87 (2008): 387, 389.

[154] "[W]e can and should maintain expectations of privacy in large quanta of personal information." David C Gray and Danielle Keats Citron, "The Right to Quantitative Privacy," *Minnesota Law Review* 98, 100 (2013).

[155] "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." Cohen, "Examined Lives: Informational Privacy and the Subject as Object" 1377.

[156] Solove, "'I've Got Nothing to Hide'and Other Misunderstandings of Privacy"; Solove, "A Taxonomy of Privacy."

[157] Martin, "Understanding Privacy Online: Development of a Social Contract Approach to Privacy."

[158] 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 exist and entry are macro norms; the real work of social contract theories is the identification and application of the actual privacy norms in the community that are developed.

Helen Nissenbaum has been consistently (and persistently) arguing for and developing a theory of privacy in public.[159] According to Nissenbaum's theory of contextual integrity, privacy is respected when norms of appropriate information flow are respected. 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. Norms of information flow for education will 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 over disclosed information.[160] 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 the privacy norms of disclosed information is different across these scholars. In fact, they do not always agree.[161] However, all argue that information is disclosed *with expectations of privacy attached* as to who

---

[159] 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." Helen Nissenbaum, "Protecting Privacy in an Information Age: The Problem of Privacy in Public," *Law and Philosophy* 17, no. 5 (1998): 559–96, 559; Nissenbaum, "A Contextual Approach to Privacy Online". "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."Kirsten Martin and Helen Nissenbaum, "Privacy Interests in Public Records: An Empirical Investigation," *Harvard Journal of Law and Technology* 31, no. Fall (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2875720. Pg. 117

[160] "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." Martin and Nissenbaum, "Privacy Interests in Public Records: An Empirical Investigation," 121.

[161] [Provide examples.] E.g., Kirsten Martin and Helen Nissenbaum, "Measuring Privacy: Using Context to Expose Confounding Variables," *Columbia Science and Technology Law Review* 18 (2017): 176–218.

will have access to this information, what uses are 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. For privacy as contextual integrity, norms of appropriate flow would dictate the expectations of information privacy based on a specific context (health care versus education versus commerce). For privacy as a social contract, the expectations of privacy are the micro norms negotiated within a defined community.

This shift from disclosed information being free from all privacy expectations to having defined privacy expectations within a particular context, community, ore 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 et al. note that privacy is not the opposite of sharing and allow for the possible benefits of sharing data yet costs of sharing data with the wrong parties.[162]

When research assumes the existence of privacy expectations of disclosed information, scholars then can measure how much respondents care about their privacy being respected around disclosed information. For example, Helen Nissenbaum and I have measured individuals nuanced expectations of privacy about who should collect location data or public records and how either will be used.[163] Katie Shilton studies individuals have strong expectations of privacy about information collected by trackers online or in apps.[164] Alice Marwick and danah boyd study teens and children expectations of privacy online.[165] Karen Levy has focused on identifying privacy of

---

[162] Costs include 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, and Wagman, "The Economics of Privacy" 462.

[163] Kirsten Martin and Helen Nissenbaum, "What Is It About Location?," *Berkeley Technology Law Journal (Forthcoming)* 35, no. 1 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3360409; Martin and Nissenbaum, "Privacy Interests in Public Records: An Empirical Investigation."

[164] Katie Shilton, "Four Billion Little Brothers?: Privacy, Mobile Phones, and Ubiquitous Data Collection," *Communications of the ACM* 52, no. 11 (2009): 48–53.

[165] Alice Marwick, "The Public Domain: Surveillance in Everyday Life," *Surveillance & Society* 9, no. 4 (2012): 378–93; Alice E Marwick and Danah Boyd, "Networked Privacy: How Teenagers Negotiate Context in Social Media," *New Media & Society* 16, no. 7 (2014): 1051–67; Marwick and Boyd.

individuals at work.[166] Even in economics, when consumer concerns are taken into consideration, scholars find that consumers need protection through regulations,[167] or find the consumers benefit from personalized pricing and promotion when given control over what data is disclosed to the targeting firm[168] or find the seller is better off not using personalized pricing.[169] In criminal law we see a shift to acknowledge the expectations of privacy for disclosed information.[170]

In many ways, the governance of information in the commercial space has fallen behind other areas by relying on privacy-as-concealment, thereby allowing the situation we find ourselves in: 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.[171]

---

[166] Karen EC Levy, "The Contexts of Control: Information, Power, and Truck-Driving Work," *The Information Society* 31, no. 2 (2015): 160–74.

[167] "[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 when these three conditions are not met, that is, when few competitors exploit unwary consumers through personalized pricing." Hoffmann et al., "Hypertargeting, Limited Attention, and Privacy: Implications for Marketing and Campaigning" 5. See also Johnson, "Targeted Advertising and Advertising Avoidance."

[168] S Nageeb Ali, Greg Lewis, and Shoshana Vasserman, "Voluntary Disclosure and Personalized Pricing," 2020, 537–38. The authors examine "what happens when consumers fully control their data—not only whether they are tracked, but what specific information is disclosed to firms" and find consumers benefit from personalized pricing when given control over what information they disclose.

[169] CHECK THIS QUOTE: I obtain two main findings. First, the seller is better off by committing to not use consumer information to set prices. This commitment encourages the consumer to disclose information that is useful for providing accurate recommendations. I show that under a mild condition, the seller's gain from accurate recommendations can exceed the loss from not being able to price discriminate. The result contrasts with the classical theory of third- degree price discrimination." Shota Ichihashi, "Online Privacy and Information Disclosure by Consumers," *American Economic Review* 110, no. 2 (2020): 569–95.

[170] 16-402 Carpenter v. United States (06/22/2018), No. No. 16-402 (Supreme Court of the United States 2017).

[171] "That stream of work [reliant on Posner and Stigler] emphasized the challenges in understanding reasons to regulate privacy when information flows should create efficiencies." Goldfarb, "What Is Different about Online Advertising?" 123.

V. HOW TO GOVERN MANIPULATION ONLINE

Targeted manipulation online undermines the authentic choice of consumers in the market. Online firms now have the knowledge of individuals' vulnerabilities as well as the reach to covertly undermine a target's decision. The economic anomaly, however, is not that one market actor knows the vulnerabilities to undermine another's decisions. When someone is in a position to manipulate—in a position to exploit the relative vulnerabilities or weaknesses of a target in order to usurp their decision making—negotiated safeguards force their interests to be aligned and punish acts that are seen as out of alignment of the target (joint ventures, NDAs, professional obligations, etc).[172] Instead, the economic anomaly here is that a market actor has the knowledge and reach to manipulate another without safeguards in place. I turn now to propose how we might minimize manipulation online and protect the authentic choice of consumers, the efficiency of transactions, and the legitimacy of the market through such safeguards.

Importantly, firms are now in this 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. Others have shown that our current policy approach in the U.S., focusing on the disclosure of information with adequate notification, does not work.[173] However, I have argued here that the

---

[172] As Posner notes, we regularly govern manipulation that undermines choice, such as when negotiating contracts under duress or undue influence or when contractors act in bad faith, opportunistically, or unconscionably. Posner, "The Law, Economics, and Psychology of Manipulation."

[173] The argument that mere notification does not work has been around for years with many attempts to have notification work better. Lorrie Faith Cranor et al., "Are They Worth Reading? An in-Depth Analysis of Online Advertising Companies' Privacy Policies," 2014; Kirsten Martin, "Transaction Costs, Privacy, and Trust: The Laudable Goals and Ultimate Failure of Notice and Choice to Respect Privacy Online," *First Monday* 18, no. 12 (2013); Kirsten Martin, "Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online," *Journal of Public Policy & Marketing* 34, no. 2 (2015): 210–27, http://dx.doi.org/10.1509/jppm.14.139; Kirsten Martin, "Do Privacy Notices Matter? Comparing the Impact of Violating Formal Privacy Notices and Informal Privacy Norms on Consumer Trust Online.," *Journal of Legal Studies* 45, no. S2 (2016): 191–215; Hirsch, "From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics"; More recently, scholars have started to move on to argue for more

disclosure of information, even with privacy notices, does not *matter* to whether privacy expectations exist. Focusing on mere 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. And, scholars and legislators have begun designing more substantive laws about how information flows online rather than process rules about adequate notification and choice of consumers.[174]

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. I make two unique suggestions which I explore more below. 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, I argue that 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

---

substantive laws around privacy and information flows seemingly giving up on notification as a useful tool. See: Solon Barocas and Helen Nissenbaum, "On Notice: The Trouble with Notice and Consent," 2009, 12–13; Waldman, "Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'"; Danielle Keats Citron and Mary Anne Franks, "Criminalizing Revenge Porn," *Wake Forest L. Rev.* 49 (2014): 345; Neil M Richards and Woodrow Hartzog, "Taking Trust Seriously in Privacy Law," *Stan. Tech. L. Rev.* 19 (2016): 431–72; Priscilla M Regan, "A Design for Public Trustee and Privacy Protection Regulation," *Seton Hall Legislative Journal* 44, no. 3 (2019): 3.

[174] Exemplary calls have been made for more due process around consumer data based decisions. Kate Crawford and Jason Schultz, "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms," *Boston College Law Review* 55, no. 1 (2014): 93; Danielle Keats Citron, "Technological Due Process," *Wash. UL Rev.* 85 (2007): 1249; Danielle Keats Citron and Frank Pasquale, "The Scored Society: Due Process for Automated Predictions," *Washington & Lee Law Review* 89 (2014); Senator Brian Schatz's proposed Data Care Act of 2018.

but also because the target's decision is modified in a way that is not known to the target by definition.[175] The difficulty in identifying manipulation from the perspective of the target (or others) makes regulating specific acts or relying on consumers to identify manipulation in the market untenable.[176]

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

1. customer facing websites and apps to gain the trust of the individual,
2. trackers to gather the data from the websites/apps,
3. data aggregators and brokers to aggregate and create intimate knowledge that expose vulnerabilities,
4. ad networks to identify the potential targets and place manipulative content, and
5. customer facing websites and apps to lure the potential targets for the manipulation.

Previous attempts to identify and regulate manipulation have assumed the data collector and manipulator were a single actor with a relationship with the target.[177] Additional pressure on consumer facing firms is warranted but can lead to firms outsourcing bad behavior to third parties which can operate outside legal and market forces. Any policy to regulate targeted manipulation will need to address each actor for their role and potential divergent interest.

Third, data traffickers—who collect, aggregate, and sell consumer data—are the engine of manipulation of online consumers, yet they have no interaction, contract, or agreement with individuals.[178] Similarly, the U.S. reliance on notice-and-choice fails to address targeted manipulation because the majority of the work done to manipulate is done by market actors without

---

[175] Wilkinson, "Nudging and Manipulation." 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.

[176] Spencer rightly points out the hurdles to regulating manipulation to include problems with identification, identifying causation and harm, and practical enforcement issues. Spencer, "The Problem of Online Manipulation."

[177] For example, solutions focused on a fiduciary duty based on an existing relationship would miss the work done by data aggregators, trackers, and ad networks. Balkin, "Information Fiduciaries and the First Amendment," 2015; Khan and Pozen, "A Skeptical View of Information Fiduciaries"; Richards and Hartzog, "Taking Trust Seriously in Privacy Law." Balkin, "Information Fiduciaries and the First Amendment," 2015.

[178] As noted by Gu et al., "If data are considered the fuel of the digital economy, 'data brokers' are its catalyst." Gu, Madio, and Reggiani, "Data Brokers Co-Opetition" 2.

a relationship with the individual and without a need to notify or gain consent.[179]

B. Curtailing Manipulation Online

When manipulation is analyzed broadly, along with A/B testing, 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."[180] However, here I have focused on targeted manipulation as the covert leveraging of a specific target's vulnerabilities to steer their decisions to the manipulator's interests. I have positioned targeted manipulation 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.[181]

In general, targeted manipulation can be governed by diminishing any of the key facets of manipulation identified above: by aligning the interests of firms and individuals, by protecting the vulnerabilities of consumers, and by decreasing the degree the tactic is hidden. Previous proposals have focused on protecting vulnerabilities and decreasing the hiddenness of manipulation. These are important and included below. I spend more time exploring how the interests of the individual can be aligned with those that collect and use their individualized data.

1. Aligning Interests

The majority of the work to manipulate goes on behind the scenes where individuals have no influence and their interests do not need to be taken into account.[182] 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

---

[179] This includes the newer California law (CCPA) because the law's restrictions on selling to third parties does not include trackers who collect data for data traffickers.

[180] Spencer, "The Problem of Online Manipulation" 985; See also Kilovaty, "Legally Cognizable Manipulation," 2019; Calo, "Digital Market Manipulation."

[181] Calo, "Digital Market Manipulation."; Daniel Susser, Beate Roessler, and Helen Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World," *Georgetown Law Technology Review, Forthcoming*, 2018; Spencer, "The Problem of Online Manipulation."

[182] Reference econ lit not taking it into consideration. CITE

that lacks transparency and therefore harms the data subjects in uncontrollable ways."[183] In fact, our current approach to focus on consumer notification and choice provides a shield for data traffickers to collect and use individuals' data without governance.[184]

Without any market pressures, data traffickers who hold intimate knowledge of individuals should be held to a fiduciary-like standard of care for how their data would be used. This would mean data traffickers would be responsible for how their products and services were used to possibly undermine the interests of the individuals. Balkin and others have called for fiduciary duties for firms that gather, aggregate, and use individualized data[185] such as duties of care, confidentiality, and loyalty[186] as well as discretion, honesty, and protection,.[187]

However, attempts to add information fiduciary duties have come under criticism for relying on the relations of trust between consumers and firms as a basis for the obligations of care over data. This has placed scholars in a bind: relying on relationships of trust focuses on customer-facing firms who

---

[183] Kilovaty, "Legally Cognizable Manipulation" 486, 2019. See also Hirsch Hirsch, "From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics."

[184] "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 shields secondary recipients of personal data, many of whom do not disclose information about their activities at all." Julie Cohen, *The Inverse Relationship between Secrecy and Privacy*, 77 SOC. RES.: AN INT'L Q. 883, 886 (2010).

[185] Ian Kerr began the discussion on additional duties on service providers based on their relationship with consumers. Richards and Hartzog have also consistently called for additional obligations of loyalty on firms with an informational relationship with consumers. 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, "Information Fiduciaries and the First Amendment" 1186, 2015. This is similar to Ido's focus on the fiduciary duties around security breaches. Kilovaty, "Legally Cognizable Manipulation," 2019; Richards and Hartzog, "Taking Trust Seriously in Privacy Law"; Richards and Hartzog, "A Duty of Loyalty for Privacy Law"; Kerr, "The Legal Relationship between Online Service Providers and Users."

[186] Fabienne Peter, "Choice, Consent, and the Legitimacy of Market Transactions," *Economics & Philosophy* 20, no. 1 (2004): 1–18.; Jack M Balkin, "Information Fiduciaries and the First Amendment," *UCDL Rev.* 49 (2015): 1183.

[187] Balkin focuses on duties with online service providers and Richard and Hartzog call for confidentiality to extend do vert new relationships. Schatz's Data Care Act is similarly situated. Balkin, "Information Fiduciaries and the First Amendment," 2015; Richards and Hartzog, "Taking Trust Seriously in Privacy Law."

have some data but are not the major drivers of data trafficking we find online. This then leaves data traffickers as having no obligations or duties of care since there are no relationships with consumers. Consumers are critical to most obligations of care or fiduciary relationships since a specific harm to a consumer is the trigger for a violation, and the consumer is responsible for identifying violations. Yet consumers are unaware of manipulation online.

I resolve these problems by placing a duty of care on data traffickers that is independent of any harms or consumer relationships. Internal and external auditors would enforce the principles identified in the duty of care. This duty of care would hold all firms that hold individualized data to data integrity principles. Such companies would be required to abide by GAAP-like regulations that are governed annually by a team of auditors to make sure their actions are aligned with the interests of consumers about whom they hold intimate data.[188] Audits are useful to ensure companies are held to a professional standard, which maintains the integrity of the industry when consumers are not in a position to correct bad behavior in the market. This shifts from focusing on consumers to identify transgressions, which has been shown to be burdensome or impossible given the information asymmetries,[189] to requiring internal and external governance to ensure these duties of care are respected. This 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.[190]

A GAAP-like governance structure could be flexible enough to understand the market needs while still being responsive to protect individual rights and concerns. And, the audit of those holding individualized data will require the firm to record and save how they use the information as well as a professional data scientist to run point on the audit. These measures provide pressure to align the interests of data aggregators with those individuals they are targeting. The justification for adding additional safeguards to entities who hold dangerous products or place individuals in a vulnerable position is well established. Firms wishing to take investor money must be audited.

---

[188] McGeveran calls for a GAAP like approach for data security. Here we would have the same idea for data protection where standards are set and others must be certified to abide by them. William McGeveran, "The Duty of Data Security," *Minn. L. Rev.* 103 (2018): 1135.

[189] Acquisti et al. working paper. They identify the problems with the extraordinary responsibilities placed on consumer in safeguarding their data online ("responsibilization").

[190] CITE.

Companies in heavy manufacturing must abide by EPA regulations. Banks have extensive reporting requirements, which were increased in the wake of the 2008 financial crises. Insurance carriers are regulated at the state level. Certain industries that have been shown to put individuals in a vulnerable position – where the market is unable to adequately police bad business practices – take on additional safeguards that are then ensured by third parties, including government agencies and auditors.

Second, customer-facing firms, such as websites and apps who have a relationship with users, need to be responsible for who they partner with and make sure the consumers' interests are respected and in alignment with all future uses of the data. Woody Hartzog and Neil 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."[191] In fact, calls for fiduciary duties are based on relationships of trust and confidence with customer-facing firms.[192]

Previously, the obligation of consumer facing firms has focused on what those consumer facing firms did themselves with the data they collected.[193] Here I extend the obligations identified by others to include ensuring the third parties invited to track and target their users abide by the same duties of care and loyalty of the consumer facing firms. If the first proposal is adopted, consumer facing firms would need to ensure all third parties pass their audit and their practices match the consumer facing firms' obligations to their users. This would prevent consumer facing firms from outsourcing bad data practices to third parties.

---

[191] Woodrow Hartzog and Neil Richards, "Privacy's Constitutional Moment and the Limits of Data Protection," *Boston College Law Review* 61, no. 5 (2020): 1687, 1745.

[192] "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." Balkin, "Information Fiduciaries and the First Amendment," 1223, 2015.

[193] For example, Prfoessors Richards and Hartzog argue that firms have an obligation of loyalty if (1) trust is invtited within an informational relationship, (2) by a firm with power over an individual, (3) and that has control over the consumers mediated experiences, and (4) where the weaker party (consumer) relies on trust of that firm. This duty of loyalty impacts what the firm can do with the consumer's information. Richards and Hartzog, "A Duty of Loyalty for Privacy Law."

Holding customer facing firms responsible for how their partners (third party trackers) gather and use their users' data would be similar to calls to extend confidentiality of user information over new relationships (not only the customer facing website) by Richards and Hartzog[194] or McGeveren's call for collectors of consumer data to ensure third parties abide by security standards[195] This would force the customer facing firm, with whom the individual has some influence, to make sure its users' interests are being respected by the third party trackers and ad ntowowkrs and marketers they invite the track and target their users.[196]

Holding a company responsible for their third party relationships is not new. Professor McGeveran calls companies to be responsible for the security of their partners within a duty of data custodians.[197] Professor McGeveran likens the duty of security being extended to third parties to a HIPAA security rule that requires business to specify security duties of their partners.[198] Similarly, payment card brands use contracts to require all data custodians in their system to comply with industry data security standards.[199] Contracts like these, which impose security obligations, are enforceable in court.[200] 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 duties of care.

In addition, consumer facing websites and apps would be similarly responsible for what third parties, such as ad networks and marketers, they allow to target their users with manipulative content. The customer facing website and apps are uniquely positioned to know and control which third

---

[194] Richards and Hartzog, "Taking Trust Seriously in Privacy Law."

[195] McGeveran, "The Duty of Data Security."

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

[197] The duties "impose a special duty on these data custodians. They must dedicate systematic effort toward the safekeeping of the personal information they hold." P. 1140. McGeveran, "The Duty of Data Security."

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

[199] William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1166 (2019).

[200] *Id.* at 1175.

part ad networks and marketers 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.[201] We can also look closer to home. Most universities have extensive agreements managing the actions of third-party recruiters they bring onto campus to hire their students. Just as universities have an obligation of care over the students they bring to campus, websites and apps have a duty of care to protect individuals from third parties whose interests may not align with the users.[202]

Customer 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 data to data traffickers and later to hold users in place for data traffickers to manipulate a target covertly. Put this way, not enough attention has been given to the role of customer facing firms in choosing the third parties that track and target their users. In fact, focusing primarily on consumer facing firms' data practices would allow them to outsource their bad data practices to ungoverned third parties who are outside the reach of market or regulatory forces.[203]

Importantly, this approach to align interests rather than limit use of data avoids two persistent problems in regulating information flows online. First attempts to limit the use of data run into first amendment critiques.[204] If the

---

[201] 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 July 20, 2020).

[202] Trademark law provides another example of a company being responsible for the questionable behavior of their third party partners. A defendant can be indirectly liable for trademark infringement if it (1) "intentionally induce[d] another to infringe" or (2) "continue[d] to supply its product to one whom it kn[ew] or ha[d] reason to know [was] engaging in trademark infringement." Inwood Labs. v. Ives Labs., 456 U.S. 844, 854 (1982). With large service providers, such as eBay, the service provider must have more than just general knowledge that its service is being used to infringe, but it cannot be willfully blind. Tiffany (NJ) Inc. v. eBay, Inc., 600 F.3d 93 (2nd Cir. 2010), cert denied, 562 U.S. 1082 (2010). This would mean that ignoring the questionable behavior of partners *on purpose* is not a legitimate defense.

[203] The outsourcing of bad business practices has a long history. Garment and manufacturing can outsource poor labor practices to other countries. Outsourcing need not be to other countries, a manufacturer may build in a non-union state to avoid union rules (Boeing's move to the southeast) or retailers may outsource cleaning staff and maintain plausible deniability as to the poor labor practices.

[204] Jane Bambauer, "Is Data Speech," *Stan. L. Rev.* 66 (2014): 57; Jane R Bambauer,

flow of information is taken as a given or legitimate, regulators have an uphill battle limiting what a company can say with that data.[205] Second, designating a use as "unfair" usually relies on a discernable *harm* to the consumer in order to trigger the regulation or law.[206] For example, the FTC's unfairness doctrine or the unfairness protections in consumer protection or even recent calls for a data protection act.[207] But the harms from manipulation are not the kind normally identified by regulators or are so dispersed as to be difficult to identify.[208] The approach proposed here does not rely on a consumer to identify a specific harm to trigger an investigation into problematic use of data.[209]

2. Protecting Vulnerabilities

Manipulation is only possible because someone—here it is data brokers—has intimate knowledge of individuals as to what renders them vulnerable in their decision making. Another tactic to regulate manipulation is to limit the collection and use of intimate knowledge by firms to manipulate consumers. A number of scholars have proposed greater protections on types of data such

---

"The Relationships between Speech and Conduct," *UC Davis Law Review* 49 (2016): 16–16.

[205] CITE Pharma case.

[206] Calo, "Digital Market Manipulation."

[207] Hirsch, "From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics"; Daniel J Solove and Woodrow Hartzog, "The FTC and the New Common Law of Privacy," *Columbia Law Review* 114 (2014): 583–676; Kilovaty, "Legally Cognizable Manipulation," 2019. 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).

[208] Calo, "Digital Market Manipulation."; Kilovaty, "Legally Cognizable Manipulation," 2019.

[209] Others leave open the idea that the FTC could regulate data practices based on procedural issues such as Citron and Pasquale. Citron and Pasquale, "The Scored Society: Due Process for Automated Predictions." 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. From Hirsch "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."" Hirsch, "From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics."

as intimate data, inferences drawn from data,[210] and sensitive information.[211] Professor Hirsch broadens what could be considered vulnerable in noting that surface information becomes problematic through predictive analytics.[212] By curtailing the collection of information at the source with the idea that consumer data that is not collected can also not be used against them.[213] Others have focused on limiting the use of information and attempted to identify problematic instances such as unfair practices, unreasonable self-dealing, and breaches of loyalty and confidentiality.[214]

3. Reducing Hiddenness

Finally, manipulation works because the tactic is hidden from the target. One way to undermine the effectiveness of manipulation is to make the type of intimate knowledge used in targeting obvious and public.[215] This could mean a notice (e.g., "this ad was placed because the ad network believes you are diabetic") or a registry when hyper-targeting is used to allow others to analyze how and why individuals are being targeted. Registering would be particularly important for political advertising so that researchers and regulators can identify the basis for hyper-targeting and identify possible manipulation.

C. Specific Policy Suggestions Across Regulations

The suggestions above would entail a new governance structure to ensure data traffickers safeguard the individualized data and align their interests with the consumers. To enforce new privacy regulations, some

---

[210] Sandra Wachter and Brent Mittelstadt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI," *Columbia Business Law Review*, 2019.

[211] Ohm, "Sensitive Information."

[212] Hirsch, "From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics."

[213] Susser, Roessler, and Nissenbaum, "Technology, Autonomy, and Manipulation"; Kilovaty, "Legally Cognizable Manipulation," 2019.

[214] Hirsch, "From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics"; Balkin, "Information Fiduciaries and the First Amendment," 2015; Hartzog and Richards, "Privacy's Constitutional Moment and the Limits of Data Protection"; Eliza Mik, "The Erosion of Autonomy in Online Consumer Transactions," *Law, Innovation and Technology* 8, no. 1 (2016): 1–38.

[215] Quote from Calo about hiddenness of manipulation

call for expanding the FTC's current scope,[216] while Regan calls for a new regulatory agency within the Commerce department.[217]

However, across privacy regulations, the following steps could be taken to 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 GDPR. For example, an individual has a right to the restriction of information processing dependent on the legitimate grounds of the controller. Yet, legitimate interests are broadly construed and the manipulation of individuals has not been identified as diminishing a human right. 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.[218]

In addition, all regulators should expand the types of information requiring additional protection in order to protect the vulnerabilities of users 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 than the inferences drawn about individuals based on that data.[219]

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 CCPA has restrictions on selling to third parties but does not include trackers who collect data for data traffickers. And, "the CCPA requires a business to provide notice if it is

---

[216] Solove and Hartzog, "The FTC and the New Common Law of Privacy"; Hirsch, "From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics."

[217] Regan, "A Design for Public Trustee and Privacy Protection Regulation."

[218] Professor 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," *Yale JL & Tech.* 5 (2002): 1.

[219] Hirsch, "From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics"; Wachter and Mittelstadt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI."

'using personal information collected for additional purposes.' This rule doesn't stop companies from using data for new purposes—it just requires disclosure if they do so." [220]

CONCLUSION

In sum, this paper 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 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. Where scholarship has focused on identifying instances of manipulation to regulate, I argue 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.

[220] Chandler et al. "Catalyzing Privacy Law" pg. 20.