Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 33 *XXXIII*
Number 2

Article 1

2023

Manipulating, Lying, and Engineering the Future

Michal Lavi

Follow this and additional works at: https://ir.lawnet.fordham.edu/iplj

Recommended Citation

Michal Lavi, *Manipulating, Lying, and Engineering the Future*, 33 Fordham Intell. Prop. Media & Ent. L.J. 221 (2023).
Available at: https://ir.lawnet.fordham.edu/iplj/vol33/iss2/1

This Article is brought to you for free and open access by FLASH: The Fordham Law Archive of Scholarship and History. It has been accepted for inclusion in Fordham Intellectual Property, Media and Entertainment Law Journal by an authorized editor of FLASH: The Fordham Law Archive of Scholarship and History. For more information, please contact tmelnick@law.fordham.edu.

Manipulating, Lying, and Engineering the Future

Cover Page Footnote

* Michal Lavi Ph.D (Law) Research Fellow at the Hadar Jabotinsky Center for Interdisciplinary Research of Financial Markets, Crises and Technology. I thank Emily Cooper for thoughtful comments and excellent editorial work. Special thanks are due to Eleesya Cordes, Grace A. Sullivan, Aaron Bondar, Caitlyn Fontana, Frances McDonald, Sarah Ishikawa, Josephine M. Luck, Abigail Ryckman, Steven Ari Halpern, Olivia Santiago, Max Fishman, Eric Mason, Martina Ferrarazzo, and their colleagues on the Fordham Intellectual Property, Media & Entertainment Law Journal staff for their great dedication, remarkable feedback, comments, suggestions, and outstanding editorial work that profoundly improved the quality of this Article. I dedicate this Article to the memory of my mother—Aviva Lavi—who died suddenly and unexpectedly. My mother taught me to love knowledge and gave me the strength to pursue it. She will always be loved, remembered, and dearly missed.

This article is available in Fordham Intellectual Property, Media and Entertainment Law Journal:
https://ir.lawnet.fordham.edu/iplj/vol33/iss2/1

Manipulating, Lying, and Engineering the Future

Michal Lavi*

Decision-making should reflect personal autonomy. Yet, it is not entirely an autonomous process. Influencing individuals' decision-making is not new. It is and always has been the engine that drives markets, politics, and debates. However, in the digital marketplace of ideas the nature of influence is different in scale, scope, and depth. The asymmetry of information shapes a new model of surveillance capitalism. This model promises profits gained by behavioral information collected from consumers and personal targeting. The Internet of Things, Big Data and Artificial Intelligence open a new dimension for manipulation. In the age of Metaverse that would be mediated through virtual spaces and augmented reality manipulation is expected to get stronger. Such manipulation could be performed by either commercial corporations or governments, though this Article primarily focuses on the former, rather than the latter.

Surveillance capitalism must depend on technology but also on marketing, as commercial entities push their goods and agendas unto their consumers. This new economic order presents benefits in the form of improved services, but it also has negative

* Michal Lavi Ph.D (Law) Research Fellow at the Hadar Jabotinsky Center for Interdisciplinary Research of Financial Markets, Crises and Technology. I thank Emily Cooper for thoughtful comments and excellent editorial work. Special thanks are due to Eleesya Cordes, Grace L. Sullivan, Aaron Bondar, Caitlyn Fontana, Frances McDonald, Sarah Ishikawa, Josephine Luck, Abigail Ryckman, Steven Halpern, Olivia Santiago, Max Fishman, Eric Mason, Martina Ferrarazzo, and their colleagues on the Fordham Intellectual Property, Media & Entertainment Law Journal staff for their great dedication, remarkable feedback, comments, suggestions, and outstanding editorial work that profoundly improved the quality of this Article.

I dedicate this Article to the memory of my mother—Aviva Lavi—who died suddenly and unexpectedly. My mother taught me to love knowledge and gave me the strength to pursue it. She will always be loved, remembered, and dearly missed.

consequences: it treats individuals as instruments; it may infringe on individuals' autonomy and future development; and it manipulates consumers to make commercial choices that could potentially harm their own welfare. Moreover, it may also hinder individuals' free speech and erode some of the privileges enshrined in a democracy.

What can be done to limit the negative consequences of hypermanipulation in digital markets? Should the law impose limitations on digital influence? If so, how and when? This Article aims to answer these questions in the following manner:

First, this Article demonstrates how companies influence decisions by collecting, analyzing, and manipulating information. Understanding the tools of the new economic order is the first step in developing legal policy that mitigates harm.

Second, this Article analyzes the concept of manipulation. It explains how digital manipulation differs from traditional commercial influences in scope, scale, and depth. Since there are many forms of manipulation, an outright ban on manipulation is not possible, nor is it encouraged since it could undermine the very basis of free markets and even free speech. As a result, this Article proposes a limiting principle on entities identified in literature as "powerful commercial speakers," focusing on regulating lies and misrepresentations of these entities. This Article outlines disclosure obligations of contextual elements of advertisements and imposes a duty of avoiding false information. In addition to administrative enforcement of commercial lies and misrepresentations, this Article advocates for a new remedy of compensation for autonomy infringement when a powerful speaker lies or disobeys mandated disclosure on products.

Third, this Article proposes a complementary solution for long-term effects of manipulation. This solution does not focus on the manipulation itself, but rather offers limitations on data retention for commercial purposes. Such limitations can mitigate the depth of manipulation and may prevent commercial entities from shackling individuals to their past decisions.

Fourth, this Article addresses possible objections to the proposed solutions, by demonstrating that they are not in conflict with the First Amendment, but rather promote freedom of expression.

Introduction

You might have heard that we are living in the era of hacking computers, but that's not even half the truth. In fact, we are living in the era of hacking humans. The algorithms are watching you right now. They are watching where you go, what you buy, whom you meet. Soon they will monitor all your steps, all your breaths, all your heartbeats. They are relying on Big Data and machine learning to get to know you better and better. And once these algorithms know you better than you know yourself, they can control and

> *manipulate you and you won't be able to do much about it.*[1]

Lisa Magrin, a forty-six-year-old teacher, drives regularly from her house in upstate New York at 7:00 a.m. and travels to a school fourteen miles away, staying there until late afternoon each school day. She also goes to a Weight Watchers meeting every so often, and occasionally to her dermatologist. How do we know this? Her smartphone, and the apps installed on it, revealed this information and sold it to commercial companies.[2] The private lives of individuals are an open book to companies which have access to their data.[3] They can see the places a person goes every minute of the day. Surveillance capitalism marks the new economic order of the twenty-first century.[4] Constant private surveillance and documentation of the public's behavior is the "new oil" used for commercial purposes.[5] Unlike oil, however, data is not a limited resource—it is constantly being created by end users. Facebook (Meta), Google, Xiaomi and other companies offer services in exchange for collecting and analyzing data from their end users,[6] through all manner of

---

1 YUVAL NOAH HARARI, 21 LESSONS FOR THE 21ST CENTURY 267–68 (2018).

2 *See* Jenifer Valentino DeVerias et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [https://perma.cc/435B-G3U4].

3 *See* Stuart A. Thompson & Charlie Warzel, Opinion, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html [https://perma.cc/G7KQ-27C8]; CARISSA VELIZ, PRIVACY IS POWER: WHY AND HOW YOU SHOULD TAKE BACK CONTROL OF YOUR DATA 8–16 (2020).

4 *See generally* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019) (coining the term "surveillance capitalism" and explaining its impact on commerce, free will and society).

5 Jonathan Vanian, *Why Data Is the New Oil*, FORTUNE (July 12, 2016), https://fortune.com/2016/07/11/data-oil-brainstorm-tech/ [https://perma.cc/5JX2-RZB2]; Lim Zenghao, *Data Is the New Oil and Electricity,* ASIAN SCIENTIST (Mar. 11, 2020), https://www.asianscientist.com/2020/03/features/smu-ai-ip-conference-data-new-oil/ [https://perma.cc/9T6E-T9QK].

6 *See* Debashis Sarkar, *New Xiaomi US Privacy Policy Will Collect Users' Personal Info, Financial Details and More,* GADGETS NOW (May 4, 2018), https://www.gadgetsnow.com/tech-news/new-xiaomi-us-privacy-policy-will-collect-users-personal-info-financial-details-and-more/articleshow/64026044.cms [https://perma.cc/5LP6-JDTQ] (detailing how Xiaomi Smartphones collect users' data for commercial purposes and can disclose the data to third parties in order to provide services).

algorithmic programs.[7] These private companies are not limited by Constitutional restrictions.[8] They collect information and create profiles of internet users even if these users do not use their service and even if they do not have an active account on their platforms at all.[9] The mass collection and analysis of data allows companies to draw conclusions about their users, from health status, to personality and desires.[10] For example, on March 13, 2020, Alphabet's life sciences division, Verily, announced it was developing a website to screen people for symptoms of COVID-19, draw conclusions on their health, and assign them risk scores.[11]

---

[7] *See* Alexander Tsesis, *Data Subjects' Privacy Rights: Regulation of Personal Data Retention and Erasure*, 90 COLO. L. REV. 593, 603 (2019).

[8] According to the "state action" doctrine developed by the U.S. Supreme Court, the U.S. Constitution and its individual proclaimed rights apply only to state action and not to private action. *See* The Civil Rights Cases, 109 U.S. 3, 18 (1883); *Developments in the Law: State Action and the Public/Private Distinction*, 123 HARV. L. REV. 1248, 1250 (2010).

[9] *See* Kashmir Hill, *How Facebook Figures Out Everyone You've Ever Met*, GIZMODO, (Nov. 7, 2017, 9:39 AM) https://gizmodo.com/how-facebook-figures-out-everyone-youve-ever-met-1819822691 [https://perma.cc/AB4W-JRA3]; Kashmir Hill, *Facebook Is Giving Advertisers Access to Your Shadow Contact Information*, GIZMODO (Sept. 26, 2018, 3:30 PM), https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051 [https://perma.cc/2JMZ-BZ6B]. *See also* Peter C. Ormerod, *A Private Enforcement Remedy for Information Misuse*, 60 B.C.L. REV. 1893, 1895 (2019) (explaining that ninety-two percent of the websites you visit have embedded Google trackers, so that the company knows just about every place you visit on the internet—regardless of whether you have a Google account or use any Google services); Sebastian Klovig Skelton & Bill Goodwin, *Lawmakers Study Leaked Facebook Documents Made Public Today*, COMPUTERWEEKLY (Nov. 6, 2019), https://www.computerweekly.com/news/252473540/Lawmakers-study-leaked-Facebook-documents-made-public-today [https://perma.cc/TCT3-CN34] (revealing the documents leaked by Facebook and explaining that Facebook planned to use its Android app to match users' location data with mobile-phone based station IDs to deliver "location-aware" products without user consent. Facebook also offers preferential deals to parties that share their user data with Facebook); Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. 11, 17 (2020) ("As digital companies know more about a given person, they can also know more about other people who are similar to that person or are connected to that person.").

[10] Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, THE GUARDIAN (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/ cambridge-analytica-facebook-influence-us-election [https://perma.cc/4859-Z66C].

[11] *See* Mason Marks, *Emergent Medical Data: Health Information Inferred by Artificial Intelligence,* 11 U.C. IRVINE L. REV. 995, 1004 (2021).

The collection and analysis of personal data can have benefits. However, the main goal of this new economic order is to extract users' behavioral data, including health conditions,[12] and create commodifiable profiles for advertisers who, in turn, micro-target users and sell them goods and agendas.[13] The story of Facebook and Cambridge Analytica serves as a good example of this new model.[14]

Today, tracking technology is used everywhere. These technologies are present in smart connected devices and wearables, producing data, which leaves a digital trace. The "datafication of everything"[15] gives technology companies, advertisers and retailers immediate feedback on what users are doing and allows these companies to target individuals in ways that were previously impossible.[16] Take for example Mustafa Al-Bassam, a security researcher that stepped into McDonald's and was prompted to download the fast-food restaurant's App on his phone. The timing of the request to download the App was not a coincidence; companies watch every move of their users, and monitor, analyze,[17] and target them with

---

12 *See id.* at 1007 ("[H]ealth inferences made about the deployment population may be used for a variety of purposes such as drawing conclusions about their health, designing personalized treatment programs for them, customizing targeted advertisements to them based on their health conditions."). *See also* Raina M. Merchant et al., *Evaluating the Predictability of Medical Conditions from Social Media Posts,* 14 PLOS ONE (2019).

13 *See* Jack M. Balkin, *The First Amendment in the Second Gilded Age*, BUFF. L. REV. 979, 999 (2018); *ZUBOFF*, *supra* note 4, at 94–97; Alexander Tsesis, *Marketplace of Ideas, Privacy, and Digital Audiences,* 94 NOTRE DAME L. REV. 1585, 1585 (2019).

14 *See* Cadwalladr & Harrison, *supra* note 10; Barbara Ortutay, *Report: Facebook Faces $5B FTC Fine Largest Ever in Tech,* NBC (July 12, 2019), https://www.nbcchicago.com/news/national-international/ftc-approves-roughly-5b-fine-for-facebook-report-2/1973191/ [https://perma.cc/QEV7-7L2V]; SIVA VAIDHYANATHAN, ANTISOCIAL MEDIA: HOW FACEBOOK DISCONNECTS US AND UNDERMINES DEMOCRACY 150 (2018); VELIZ, *supra* note 3, at 77.

15 *See* Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 140 (2017) ("[N]ew techniques for customer tracking, immersive social design, and data analysis all promised new possibilities for profiting from targeted marketing in an increasingly fragmented media ecosystem.").

16 *See* Joseph Turow, *Americans and Marketplace Privacy: Seven Annenberg National Surveys in Perspective*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 151 (2018); ZUBOFF *supra* note 4, at 80 ("[T]hese include websites visited, psychographics, browsing activity, and information about previous advertisements that the user has been shown, selected and/or made purchases after viewing.").

17 *See* Matt Young, *How to Stop Google Tracking Your Every Move,* NEWS.COM.AU (Mar. 17, 2017, 10:46 AM), https://www.news.com.au/technology/online/security/how-to-

messages in ways that many users would prefer to avoid.[18] After all, no one asked Mustafa whether he wanted the McDonald's App—he merely entered the restaurant, companies knew his location and targeting followed. This is an example to a basic location-based influence. As the Article demonstrated there are more sophisticated data driven influences.

Customer tracking practices existed long before anyone had a smartphone.[19] Credit cards, loyalty cards, and email addresses allowed vendors to collect customer information with ease. An analysis of this data allowed retailers to predict the needs of consumers and assign them coupons. In one well known case, Target determined that a teenager was pregnant before her father did.[20] With internet-connected devices, the possibilities of tracking consumers are far more numerous. If shoppers carry the right apps on their smartphones, beacon technologies installed in stores transmit a

---

stop-google-tracking-your-every-move/news-story/6abd14e4746da56b10ee4d58d785df80 [https://perma.cc/M2N3-X9H7] ("Yesterday I almost had a heart attack when I entered McDonald's and I had a notification on my phone asking me to install their app."); ZUBOFF *supra* note 4, at 154.

18 *See* Joseph Turow & Chris Jay Hoofnagle, *Mark Zuckerberg's Delusion of Consumer Consent*, N.Y. TIMES (Jan. 29, 2019), https://www.nytimes.com/2019/01/29/opinion/zuckerberg-facebook-ads.html [https://perma.cc/9A7K-URMR].

19 *See, e.g.*, JOSEPH TUROW, THE DAILY YOU, HOW THE NEW ADVERTISING INDUSTRY IS DEFINING YOUR IDENTITY AND YOUR WORTH 4 (2012) (focusing on tracking and profiling online "advertisers in the digital space expect all media firms to deliver to tem paticular types of individuals—and incresingly, particular individuals—by leveraging a detailed knowledge about them and their behaviors that was unheard of a few years ago . . . based in large part on measurable physical acts such as clicks, swipes, mouseovers and even voice commands."); *see generally* Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J. L. & TECH. 54, 59 (2014) (reviewing practices of personalized analysis of information, and data driven marketing that collects data on users).

20 *See* NEIL RICHARDS: WHY PRIVACY MATTERS 36 (2021); Marks, *supra* note 11, at 1004; Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did,* FORBES (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=327df41b6668 [https://perma.cc/8AXH-SW4C]; Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html [https://perma.cc/K7B3-U4YS].

signal, alerting merchants to send shoppers personalized coupons or messages associated with the goods in the beacon's proximity. [21]

Aggressive advertising and tracking is now everywhere. Sensors on smart connected devices can "understand" behavior, habits, moods, and emotions.[22] Real time analysis translates into real time action.[23] Complex personalization formulas, which evaluate a customer's shopping list and location in the store, present consumers with ideas about what to buy. They can send consumers recipes and discounts based on what is in their shopping cart, and even adapt to customers' responses to those suggestions.[24] Recently, McDonald's reached an agreement to acquire Dynamic Yield, a startup that provides retailers with machine-learning, algorithmically-driven decision logic technology.[25] In a pilot program powered by Dynamic Yield at a McDonald's restaurant in Miami, algorithms crunch data to change the menu of the restaurant based on the weather, time of day, local traffic, nearby events, and of course historical sales data, both at that specific franchise and around the world.[26]

Companies can also deduce customers' personality traits and predict what customers would like and dislike based on products the

---

[21] *See* JOSEPH TUROW, THE AISLES HAVE EYES: HOW RETAILERS TRACK YOUR SHOPPING, STRIP YOUR PRIVACY AND DEFINE YOUR POWER 1–2 (2017) ("If shoppers carry the right apps on their smartphones and have the correct technology turned on, the beacons will alert the merchants and they can send the shoppers personalized coupons or other messages associated with the goods in a beacon's proximity.").

[22] *See e.g.*, Sidney Fussell, *Alexa Wants to Know How You're Feeling Today*, ATLANTIC (Oct. 12, 2018), https:// www.theatlantic.com/technology/archive/2018/10/alexa-emotion-detection-ai-surveillance/572884/ [https://perma.cc/9LTS-E6M5]

[23] ZUBOFF *supra* note 4, at 293–94.

[24] *See* JOSEPH TUROW, THE AISLES HAVE EYES: HOW RETAILERS TRACK YOUR SHOPPING, STRIP YOUR PRIVACY AND DEFINE YOUR POWER 4 (YALE U. PRESS 2017); Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRIES L. 157, 169 (2019).

[25] This technology makes it possible to nudge shoppers adding items to their cart about what other, similar customers bought. *See* Brian Barrett, *McDonalds Bites on Big Data with $300 Million Acquisition,* WIRED (Mar. 25, 2019, 6:17 P.M.), https://www.wired.com/story/mcdonalds-big-data-dynamic-yield-acquisition/ [https://perma.cc/H54J-MNDM].

[26] *Id.* It should be noted that the menu is not uniform, but it personalizes recommendations. If someone orders two Happy Meals at 5:00 p.m., for instance, it may be a parent ordering for their kids, and thus, the personalized suggestion might be a coffee or snack for him, and he might decide to treat himself to a pick-me-up.

customer discusses on social networks.[27] They use this information to influence consumers' decision-making and enhance their profits in the process. The surveillance economy translates into socio-technical engineering in a scale never witnessed before.[28] An advertiser can identify the present emotional state of a potential consumer—whether he is sad, lonely, scared, happy or confident—and target the consumer using this information.[29] Advertisers seize the opportunity to reach a consumer when he is most susceptible, with messages that were successful with others who shared the same traits and circumstances.[30] A person trying to lose weight "by avoiding snacking between meals could receive a text on his phone from the nearest donut shop exactly when he was least likely to resist."[31] Online social network platforms exploit vulnerable youth that lack self-confidence, targeting emotions such as sadness.[32] Companies not only utilize known cognitive biases, but also exploit specific, individual vulnerabilities—or even create new ones.[33]

---

[27] TUROW, *supra* note 19; *see also* Michal Kosinski et al., *Private Traits and Attributes are Predictable from Digital Records of Human Behavior,* 110 PROC. NAT. ACAD. SCI. 5802, 5802 (2013) (explaining that a wide range of personality traits can be accurately evaluated based on an individual's Facebook likes).

[28] *See* BRETT FRISCHMANN & EVAN SELINGER, RE-ENGINEERING HUMANITY 117 (Cambridge Univ. Press 2018).

[29] *See* Tom Kelshaw, *Emotion Analytics: A Powerful Tool to Augment Gut Instinct*, THINK WITH GOOGLE (Aug. 2017), https://www.thinkwithgoogle.com/intl/en-145/marketing-strategies/data-and-measurement/emotion-analytics-powerful-tool-augment-gut-instinct/ [https://perma.cc/E3L5-U7UR]; Julie E. Cohen*, The Emergent Limbic Media System, in* LIFE AND THE LAW IN THE ERA OF DATA-DRIVEN AGENCY 60, 61 (Mireille Hildebrandt & Kieron O'Hara eds., 2020). ("The operation of the digital information environment has begun to mimic the operation of the collection of brain structures . . and that play vital roles in a number of precognitive functions, including emotion, motivation, and habit-formation.").

[30] *See* JARON LANIER, TEN ARGUMENTS FOR DELETING YOUR MEDIA ACCOUNT RIGHT NOW 6 (Macmillan 2018).

[31] Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 996 (2014).

[32] *See* Nick Whigham, *Leaked Document Reveals Facebook Conducted Research to Target Emotionally Vulnerable and Insecure Youth,* NEWS.COM.AU (May 1, 2017); Daniel Susser et al., *Online Manipulation: Hidden Influences in a Digital World,* 4 GEO. L. TECH. REV. 1, 25–26 (2019).

[33] *See* Shaun B. Spencer, *The Problem of Online Manipulation*, 2020 U. ILL. L. REV. 959, 977 (2020) ("[M]arketers could expand upon these techniques by exploiting or even triggering biases and vulnerabilities at the individual consumer level, rather than relying on biases and vulnerabilities prevalent in the general population.").

New technological tools target everyone, not just susceptible individuals. Like a Skinner's box,[34] they create conditioning rewards and reinforcement,[35] change the context of a situation,[36] and modify the behavior of individuals.[37] They are turning users into products, their activity into assets, and their platforms into "weapons of mass manipulation."[38] The metaverse and augmented reality present new opportunities to monitor users, including psychological responses and biometric data such as facial expressions.[39]

---

[34] *See* B.F Skinner, *Operant Behavior*, AM. PSYCH. 503–15 (1963); Kendra Cherry, *Skinner Box or Operant Conditioning Chamber*, VERYWELL MIND (Aug. 30, 2018), https://www.verywellmind.com/what-is-a-skinner-box-2795875 [https://perma.cc/BES5-9EZG] (explaining the "skinner box"—an apparatus that can condition behavior. In Skinner's experiments, the influence was on animals; whereas in the technological era, users find themselves in the skinner box).

[35] *See* ZUBOFF, *supra* note 4, at 322–25 ("[O]ne's notion that 'human material was changeable'—that one's personality, identity, awareness, and capacity for self-determining behavior could be crushed, eliminated, and replaced by external control—incited a new sense of panic and vulnerability.").

[36] *See* Adam D. Kramer et al., *Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks*, 111 PROC. NAT'L ACAD. SCI. 8788, 8788 (2014) (describing an experiment conducted by Facebook in which the company used algorithms to distribute specific types of content to users' feeds); *see also* FRISCHMANN & SELINGER, *supra* note 28, at 117.

[37] *See* FRISCHMANN & SELINGER, *supra* note 28, at 124; LANIER, TEN ARGUMENTS, *supra* note 30, at 28–29 (coining the acronym BUMMER—Behaviors of Users Modified and Made into an Empire for Rent—to describe the influence of social media business models on users); ZUBOFF, *supra* note 4, at 305; *see, e.g.*, Joan E. Sollsman, *YouTube's AI is the Puppet Master Over Most of What You Watch*, CNET (Jan. 10, 2018), https://www.cnet.com/tech/services-and-software/youtube-ces-2018-neal-mohan/ [https://perma.cc/44DL-X7UM].

[38] *See* Danielle Keats Citron, *Cyber Mobs, Disinformation, and Death Videos: The Internet as It Is (and As It Should Be),* 118 MICH. L. REV. 1073, 1086 (2020).

[39] Danny Friedmann, *Digital Single Market, First Stop to The Metaverse: Counterlife of Copyright Protection Wanted, in* LAW AND ECONOMICS OF THE DIGITAL TRANSFORMATION (Klaus Mathis & Avishalom Tor, eds.) (Springer, forthcoming 2022) (manuscript at 18) ("Because of its interoperability, the technology of the metaverse is able to keep tracking you. Because of its equipment that makes immersive experiences possible, the technology is able to determine where the gaze lingers, when the pupil dilates, the facial expressions, heart and respiration rate, and galvanic skin responses, etc."); *see* Louis B. Rosenberg, *Regulation of the Metaverse: A Roadmap*, PROC. 6TH INT'L CONF. ON VIRTUAL & AUGMENTED REALITY SIMULATIONS 21, 25 (2022) ("In the metaverse, consumers won't be targeted with simple pop-up ads or promo-videos that are obviously advertisements. Instead, consumers will be targeted by simulated people, products, and activities that seem just as real as everything else around us."); Scott Bloomberg, *Political Advertising in Virtual Reality*, FIRST AMEND. L. REV. (forthcoming) ("Operating a VR environment like

This Article does not deal with invasion of privacy in itself. Rather, it focuses on its results: manipulation.[40] In other words, the process *deliberately* aimed at motivating and influencing individuals to take specific steps and make decisions in a manner considered socially unacceptable.[41] It focuses on manipulation in commerce rather than political manipulation, since the harm caused by these two "types" of manipulation differ from one another,[42] even though both use similar tools.[43]

This Article asks how should the law treat manipulation in markets: should it impose limitations on digital influence that manipulates users' decisions? And if so, when and how? The article aims to provide answers by using the following structure:

Part I focuses on the lifecycle of data and identifies new strategies of influence. It lays down the first step for understanding the

---

the so-called metaverse will involve the collection, processing, storage, and sharing of vast quantities of personal data. That data will likely range from basic account information to highly-sensitive information that tracks how users interact with their virtual surroundings.").

40 *See* Karl Manheim & Lyric Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 YALE J. L. & TECH. 106, 109 (2019) ("The resulting loss of autonomy in personal decision-making has been no less serious than the loss of privacy.").

41 This Article will expand on definitions of manipulation in Part II. *See* Zarsky, *Privacy and Manipulation, supra* note 24, at 173.

42 *See* YOCHAI BENKLER ET AL., NETWORK PROPAGANDA: MANIPULATION, DISINFORMATION, AND RADICALIZATION IN AMERICAN POLITICS 30 (Oxford Univ. Press 2018) (explaining that the main harm resulting from political manipulation is to democracy, while the main harm of manipulative marketing is to welfare, consumer sovereignty, and consumer protection).

43 *Id.* at 269 (explaining that the use of psychographic information, profiling, and targeting are in fact transplanting behavioral insights from marketing to the political realm); *see also* Anthony Nadler et al., *Weaponizing the Digital Influence Machine*: *The Political Perils of Online Ad Tech*, DATA & SOC. RSCH. INST. 1, 17, 36 (Oct.17, 2018), https://datasociety.net/library/weaponizing-the-digital-influence-machine/ [https://perma.cc/9F2R-U7EJ]; Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. 335, 335 (2014); Manheim & Kaplan, *supra* note 38, at 111 (discussing the dangers of manipulation through AI to core democratic principles of privacy, autonomy, equality, the political process, and the rule of law); VAIDHYANATHAN, *supra* note 14, at 172 (referring to Facebook's custom audiences' service which allows advertisers efficient targeting); Charles Duhigg, *Campaigns Mine Personal Lives to Get Out Vote*, N.Y. TIMES (Oct. 13, 2012), https://www.nytimes.com/2012/10/14/us/politics/campaigns-mine-personal-lives-to-get-out-vote.html [https://perma.cc/E2AF-ZYQV]; *see generally* Daniel Kreiss, *Yes We Can (Profile You): A Brief Primer on Campaigns and Political Data,* 64 STAN. L. REV. 70, 70 (2012).

problem caused by companies influencing the public's decision-making patterns and behavior.

Part II draws on scholarly work and defines manipulation. It differentiates manipulation from other types of influence.[44] It argues that the digital algorithmic era has taken manipulation to a new level, changing the severity of its harm and creating unique concerns. This section explains that the law already regulates manipulation of individuals in vulnerable positions and situations.[45] It asks and answers whether advancing the concept of liability is desirable and what the scope of liability should be.[46]

Following this analysis, Part III outlines a limiting principle for legal intervention. It does not focus on technology itself, but instead proposes the regulation of lies uttered by powerful commercial speakers, interpreting lies broadly to include contextual elements of the message and not just the message itself. Accordingly, lies should include misrepresentations of contextual elements of advertisement.[47] Such lies should be regulated as they distort and subvert an individual's decision-making process and infringe *both* the autonomy and welfare of a person. Like regulation against stealth marketing in mass media, it imposes companies a duty to avoid false information and disclosure obligation of specific contextual elements of advertisements.[48]

This Article pushes further the concept of legally redressable harms in the digital age as it recognizes the actual harm of manipulation. It proposes new remedies and even compensation for infringing upon a person's autonomy when companies lie or fail to comply with the disclosure duties.

---

44 *See* Susser et al., *supra* note 32, at 32.

45 *See* Micah L. Berman, *Manipulative Marketing and the First Amendment*, 103, GEO. L.J. 496, 505 (2015); Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 449 (1978); *see also* Odorizzi v. Bloomfield Sch. Dist., 246 Cal. App. 2d 123, 127–28 (1966) (applying the doctrine of undue influence).

46 This Article addresses policy concerns and doctrinal problems of liability.

47 *See* Helen Norton, *Powerful Speakers and Their Listeners*, 90 COLO. L. REV. 441, 442 (2019)*; see also* Susser et al., *supra* note 32, at 22.

48 These obligations are promoted in political contexts. *See* BENKLER ET AL., *supra* note 42, at 368.

Manipulation can subvert decision making even if companies disclose it, as applications present choices to users based on their history on the platform, influencing future decision making. Part IV proposes a complementary solution to the problem of shackling individuals to their past decisions. It proposes limitations on data storage and retention that would apply as a default rule, even if a person consented to the collection of data in the first place.

Part V addresses procedural barriers and free speech objections to the proposed solutions.[49] It argues that new technologies at the service of companies change the nature of speech, the speakers themselves and the scope of harm that is caused. In light of these changes, there is a need to recalibrate the theory of commercial free speech. In the context of consumer protection, courts should focus on the listeners' right to information.[50] This will allow a rejection of a strict scrutiny test and returning to previous conventions of commercial free speech.[51]

I. Undue Influence in Digital Markets: A Data Lifecycle Perspective

The spread of influence depends on technology but also on legal and institutional conditions. Personal data is the key input into most economic activity.[52] Today, with the development of connected devices that surround every aspect of our lives, and with new tracking tools,[53] all aspects of everyday life are now transformed into

---

[49] 47 U.S.C. § 230(c)(1) immunizes intermediaries from liability for content created by other content providers. In addition, in recent years, the Court has applied broad First Amendment protections even in commercial contexts. *See, e.g.*, Sorrell v. IMS Health Inc., 564 U.S. 552, 573–74 (2011) (extending the protection to economic conduct in engaging with data).

[50] Norton, *supra* note 47.

[51] *See, e.g.*, Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 572 (1980).

[52] *See* Ashutosh Bhagwat, *The Law of Facebook*, 54 U.C. DAVIS L. REV. 2353, 2360 (2021).

[53] On collection of information by Internet of Things (IOT) devices see Paul Ohm & Nathaniel Kim, *Legacy Switches: A Proposal to Protect Privacy, Security, Competition, and the Environment from the Internet of Things*, OHIO ST. L.J. (forthcoming 2023) (manuscript at 5) ("Almost all [IOT] devices embed tiny computers that wirelessly connect to the internet, our smartphones, and one another. Even when everything works as planned,

quantifiable data.[54] This datafication of everything creates an environment in which a person can browse intuitively and extend his abilities.[55] Yet, in a new economic order, the datafication of everything is likely to be used for instrumental purposes.[56] In other words, companies are likely to use the information to shape behavior of individuals in order to enhance their own profits.[57]

Data harvesting and collection, data analysis, predictive profiling, and new ways of behavioral microtargeting have profoundly reshaped patterns of information flow and participation in social and commercial life.[58]

The following part highlights the unique ways that form the infrastructure for influencing consumers through the data lifecycle.

these devices contribute to a growing and pervasive surveillance society, creating a detailed record of what individuals and groups do, say, think, and feel.").

54 See Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 140 (2017) ("[T]he everyday lives of network users have become increasingly datafied—converted into structured flows of data suitable for continuous collection and analysis at the platform level."); Karin van Es, Mirko Tobias Schäfer, *Introduction: New Brave World*, *in* THE DATAFIED SOCIETY: STUDYING CULTURE THROUGH DATA 13 (2017).

55 *See, e.g.*, Joseph A. Paradiso, *Our Extended Sensoria: How Humans Will Connect with the Internet of Things*, MIT TECH. REV. (Aug. 1, 2017), https://www.technologyreview.com/2017/08/01/68061/our-extended-sensoria-how-humans-will-connect-with-the-internet-of-things [https://perma.cc/YPQ9-5QFX]; Gershon Dublon & Joseph A. Paradiso, *Extra Sensory Perception,* 311 SCI. AM. 36, 40–41 (2017).

56 ZUBOFF, *supra* note 4, at 208–09.

57 *Id.* at 8; Bhagwat, *supra* note 52 ("[T]hose who possess and control that data, primarily the major technology companies such as Google, Facebook, and Amazon, have the power to predict and manipulate a huge range of human choices.").

58 *See generally,* Cohen*, The Emergent Limbic Media*, *supra* note 29.

A. Data Collection, Harvesting and Data Storage

Every minute of every day everywhere on the planet, dozens of companies—largely unregulated, little scrutinized—are logging the movements of tens of millions of people with mobile phones and storing the information in gigantic data files.[59]

The first stage of the "data lifecycle" is data collection. In the digital age, data collection is deeper than ever before.[60] Everything we do is recorded stored and monitored. Social media and apps seduce users to share information willingly by using architecture that encourages sharing.[61] Social media apps organize everything around "friending, clicking, retweeting, responding,"[62] and sharing personal information with others.[63] Similar to the gaming industry, design and technology turn the use of social media to an inherent need.[64] Individuals become addicted to engagement, and share more information, download applications[65] and expose themselves to a

---

[59] *See* Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES: THE PRIVACY PROJECT (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html [https://perma.cc/G7KQ-27C8].

[60] *See* Daniel E. Rauch, *Customized Speech and the First Amendment*, 34 HARV. J. L. & TECH. 407, 433 (2022) (referring to the ability to collect vast, and often highly intimate, troves of digitized audience information).

[61] *See* Michal Lavi, *Targeting Exceptions*, 32 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 65, 93 (2021); Michal Lavi, *Publish, Share, Re-Tweet, and Repeat*, 54 U. MICH. J. L. REFORM 441, 461 (2021).

[62] *See* BERNARD E. HARCOURT, EXPOSED: DESIRE AND DISOBEDIENCE IN THE DIGITAL AGE 41 (2015).

[63] *Id.* at 90; Susser et al., *supra* note 32, at 25–26 ("[B]oth the information [we] knowingly disseminate about [ourselves] (e.g., when [we] visit websites, make online purchases, and post photographs and videos on social media), and the information [we] unwittingly provide as (e.g., when those websites record data about how long [we] spend reading browsing them, where [we] are when [we] access them, and which advertisements [we] click on), reveals a great deal about who [we are, what interests us, and what we] find amusing, tempting, and off-putting.").

[64] ZUBOFF, *supra* note 4, at 466 (explaining that "just as ordinary consumers can become compulsive gamblers at the hands of the gaming industry," behavioral technology draws "ordinary young people into an unprecedented vortex of social information").

[65] *See* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATION CAPITALISM 42 (2019). ("[B]ecause that project requires large numbers of users generating large amounts of data, the platform provider's goal is to become and remain the indispensable point of intermediation for parties in its target markets.");

robust system aimed primarily at collecting their data,[66] and then selling it to third parties.[67]

In addition to information that internet users actively disseminate while engaging with other users, there is also an underlying, constant collection of data on users. This data is incidental to everyday activity and is created without users' awareness, and without actively sharing the information by the user. This data can be a by-product of the interactions with others,[68]or a trail of information that is created automatically with every engagement of a person with connected devices, and captured by these devices. The social media and the web browsers we use—or accidently visit—constantly collect personal data.[69] The rapid move into a world dominated by the

---

HARCOURT, *supra* note 62, at 122 (referring to the collection of information under the metaphor of "the mirrored glass pavilion"); LANIER, *supra* note 30, at 23 (arguing that addiction stands in contrast to free will).

66 *See* LANIER, *supra* note 30, at 21 ("[A]ddiction is a big part of the reason why so many of us accept being spied on and manipulated by our information technology."); *see also* Allison Zakon, *Optimized for Addiction, Extending Product Liability Concepts to Defective Designed Social Media Algorithm and Overcoming the Communication Decency Act,* 2020 WIS. L. REV. 1107, 1115 (2020); Katie Mettler, *A Lawmaker Wants to End 'Social Media Addiction' by Killing Features that Enable Mindless Scrolling*, WASH. POST (July 30, 2019, 4:08 PM), https://www.washingtonpost.com/technology/2019/07/30/lawmaker-wants-end-social-media-addiction-by-killing-features-that-enable-mindless-scrolling/ [https://perma.cc/2UB3-4JUS].

67 *See, e.g.*, hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1202 (9th Cir. 2022) (holding that the professional networking site cannot deny HiQ Labs—a data analytic company—access to public LinkedIn profiles, and HiQ can scrape the information and data mine it).

68 *See* Solon Barocas & Karen Levy*, Privacy Dependencies,* 95 WASH. L. REV 555, 562 (2020) (explaining that an intermediary can learn about a person by virtue of his social relationships with others; reveal attributes of a person from similarities to others for whose attributes are known, or draw conclusions about how he is different than others, even if he did not actively publish information); *see also* Ari Ezra Waldman, *Privacy's Rights Trap* 117 NW. L. REV. 88, 93 (2022) ("Decisions to consent to data collection are never purely personal decisions. Instead, one person's decision to consent to sharing their information frequently implicates others sharing some sort of connection with them.").

69 Ibrahim Altaweel et al., *Web Privacy Census*, TECH. SCIENCE (Dec. 14, 2015), techscience.org/a/2015121502/ [https://perma.cc/TBW7-A6NN] (reporting that 92% of websites have embedded Google trackers, so that the company knows every other site you visit on the Internet—regardless of whether you have a Google account or use any Google services). *See* Ormerod, *supra* note 9, at 3; HARCOURT, *supra* note 62, at 1; ZUBOFF, *supra* note 4*,* at 80 (explaining that the information collected includes "websites visited, psychographics, browsing activity, and information about previous advertisements that the

Internet of Things (IoT),[70] merges individuals' online activities with their offline ones.[71] This brave new technological world enables companies to collect data online in areas traditionally perceived as offline. This scale of collection is made possible through smart connected devices, such as wearables,[72] digital assistants, smart speakers, fitness trackers, and other gadgets that include sensors.[73] These devices are always on and sense and monitor a person's speech, heart rate, blood pressure, voice,[74] and other biometric

---

user has been shown, selected and/or made purchases after viewing"); LANIER, *supra* note 30, at 5.

70 Ohm & Kim, *supra* note 53; Manheim & Kaplan, *supra* note 40, at 122; Balkin, *supra* note 13, at 991; GILAD POSNER & ERIN KENNEALLY, PRIVACY AND THE INTERNET OF THINGS, U.C. BERKELEY, CTR. LONG TERM CYBERSECURITY 5 (June 7, 2018) ("The Internet of Things emerged from a number of overlapping trends: widespread and inexpensive network access, cheap sensors and computing power, miniaturization, location positioning technology, inexpensive prototyping, and the ubiquity of smartphones as a platform for device interfaces.").

71 COHEN, *supra* note 65, at 57 ("[S]ubsequent continuing extensions of surveillance capability have been more deliberate. The primary vehicles for those extensions have been the marketplace shifts towards smart mobile devices, wearable computing, and the internet of things."). Today, sensors in physical objects collect information on individuals and their networks online and offline. *See* MIREILLE HILDEBRANDT, SMART TECHNOLOGIES AND THE END(S) OF LAW: NOVEL ENTANGLEMENTS OF LAW AND TECHNOLOGY 9, 41 (2015); VAIDHYANATHAN, *supra* note 14, at 101 (explaining that specific technologies and intermediaries interact with users' minds and bodies); *see also* Susser et al., *supra* note 32, at 20 ("[W]e need not 'go online' in the traditional sense to be digitally tracked. [Our] credit card purchases log what we buy in brick-and-mortar stores, police law enforcement license plate readers track where they drive, and facial recognition software identifies [us] as [we] move through public spaces.").

72 Marion Burland & Thierry Chevallier. *The Role of Massive Databases in the Post-Market Clinical Follow-Up of Medical Devices*, PROC. 15TH INT'L JOINT CONF. ON BIOMEDICAL ENG'G SYS. AND TECHS. 247–48 (Feb. 2022), https://hal.archives-ouvertes.fr/hal-03656831/file/109526.pdf [https://perma.cc/K2GS-M5W9] ("Wearable devices that include connected bracelets and watches, sensors or any other medical device collect information through consumer and patient declarations and also passively. This passive, automated collection of information from sensors is done directly with interfaces connected to databases that concentrate information from various sources and of various types.").

73 Posner & Kenneally, *supra* note 70, at 5 (listing examples of the incredible range of products that comprise the IoT).

74 *See* Nick Couldry & Joseph Turow, *Market-Driven Voice Profiling: A Framework for Understanding*, 23 ADVERTISING & SOC'Y Q. (2022); Nils S. Borchers, Book Review, 22 STUDIES IN COMMC'N SCI. 273, 273 (2022) (reviewing JOSEPH TUROW, THE VOICE CATCHERS: HOW MARKETERS LISTEN IN TO EXPLOIT YOUR FEELINGS, YOUR PRIVACY, AND

information.[75] Furthermore, the age of Metaverse that merges offline and online by using virtual and augmented reality tools, allows collection of unique information on users, their movements, their facial expressions, vocal inflections, and vital signs, allowing to predict users' emotional state.[76]

Even if a person does not use one of these devices and is not a member of an online social network, web-connected surveillance cameras, smart billboards, in-store retail tracking systems, and other public technologies are observing his movements and habits, resulting in the collection and amalgamation of his data on a massive scale.[77] Individuals are left in the dark on the collection of their data, and they do not know in whose hands it is stored and analyzed.[78] Moreover, companies can collect data for one purpose and share with third parties for other purposes, without users' awareness. The recent Facebook leak serves as an example.[79] A person can share information with an App and it transfers it to Facebook.[80]

YOUR WALLET (2021)) ("The industry is united by its interest in using voice as another source for collecting biometrical data.").

75 *See* Heather Kelly, *How an Alexa Speaker Recorded and Shared a Private Conversation,* CNN (May 24, 2018, 7:43 PM), https://money.cnn.com/2018/05/24/technology/alexa-secret-recording/index.html [https://perma.cc/JYF6-P5HK] (discussing how Amazon Alexa listens to everything we say); s*ee, e.g.*, Geoffrey A. Fowler, *Alexa Has Been Eavesdropping on You This Whole Time*, WASH. POST (May 6, 2019, 9:00 AM), https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/ [https://perma.cc/464T-UV66]; *see also* Ormerod, s*upra* note 9, at 3 ("The devices in your home are listening to you and sometimes send recordings of your conversations to your acquaintances.").

76 *See* META, INTRODUCING META: A SOCIAL TECHNOLOGY COMPANY (Oct. 28, 2021), https://about.fb.com/news/2021/10/facebook-company-is-now-meta/; Louis B. Rosenberg, *supra* note 37, at 24.

77 TURO, *supra* note 24, at 123 ("[A company] installed cameras with 3D sensors in stores to track shopper activity in proximity to goods made by the company's client."); Posner & Kenneally, *supra* note 70, at 7.

78 VAIDHYANATHAN, *supra* note 14, at 67 (explaining that, unlike the concept of panopticon demonstrated by Jeremy Benthham, today's surveillance of the individual is conducted by all). Vaidhyanathan coins the concept of Crypticon, a type of surveillance that is ubiquitous yet even its very existence is supposed to be hidden from clear view. *Id.*

79 *See* Tsesis, *supra* note 7.

80 Calo, *supra* note 31, at 1004; *see, e.g.*, Sam Schechner &, Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, WALL ST. J. (Feb. 22, 2019, 11:07 AM), https://www.wsj.com/articles/you-give-apps-sensitive-personal-

In some cases, users give their consent for their data to be collected; some companies even pay for the right to collect users' information.[81] Yet, even if individuals consent to massive surveillance of smart devices and apps, it is not informed consent.[82] While the user might have an illusion that he has choice to consent, and control over his information, this choice is only technical and it shifts the burden to protect privacy from the companies to the user.[83] This shift occurs, among other things, when the owners of the online platforms require users to sign or accept a pre-written "privacy policy." Yet, designs of websites can be misleading and even abusive, the term "privacy policy" is in itself misleading, and it is difficult to gain meaningful consent.

---

information-then-they-tell-facebook-11550851636 [https://perma.cc/CWT3-U2DW]; *see also* Sarkar, *supra* note 6; FRISCHMANN & SELINGER, *supra* note 28, at 35.

81 *See, e.g.*, Kari Paul, *Facebook Launches App That Will Pay Users for Their Data*, GUARDIAN (June 12, 2019, 9:21 PM), https://www.theguardian.com/technology/2019/jun/11/facebook-user-data-app-privacy-study [https://perma.cc/J3BN-JQ9Q] (highlighting an app that allows users to sell Facebook data on how they use competitors' apps). In many cases, companies collect data or share data with third parties without consent. *See* ZUBOFF, *supra* note 4, at 139–40 (giving an example of the practices of Google's street view, which collected personal information via Wi-Fi and the use of cameras); Timothy Libert, *Exposing the Invisible Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites,* 9 INTELL. J. COMMC'N 3544, 3548 (2015).

82 *See* ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA AND CORPORATE POWER 53 (2021); ZUBOFF *supra* note 4, at 48–51. Many users believe that privacy policies mean their data is protected, even though it is just a statement of data use. *See* Joseph Turow et al., *Persistent Misperceptions: Americans' Misplaced Confidence in Privacy Policies*, 62 J. BROAD. & ELEC. MEDIA 461, 461 (2018). In addition to the cognitive biases of users, surveillance capitalism entities exacerbate the problem as they manipulate users' consent by design. *See* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 21–54 (2018) [*hereinafter* HARTZOG, PRIVACY'S BLUEPRINT]; Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent,* 96 WASH. U. L. REV. 1461, 1476–91 (2019) (referring to three types of consent that are not meaningful: unwitting consent, coerced consent and incapacitated consent and dubbing them "the pathologies of consent.").

83 *See* Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 811 (2019) ("Choice, though technically required by even supposedly strict laws like the GDPR, becomes an easy tactic for shifting the burden of privacy management from the technology company, which is actually well-situated to address privacy issues efficiently, to the user, who is not.").

Online platforms are designed to appear trustworthy to users, reducing their resistance to sharing personal information.[84] Designers make certain stylistic choices to confuse users, so they find it difficult to express their actual preferences.[85] For example, website designers hide opt out buttons, or frame specific choices,[86] triggering cognitive biases, "that encourage us to give up and cede control over our privacy."[87] Several studies have identified many interface designs that coerce users to consent to data collection without understanding the consequences.[88] For instance, a designer may make the

---

[84] *See* Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox*', 31 CURRENT OP. PSYCH. 105, 108–09 (2020).

[85] *See* Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43 (2021); *see also* WALDMAN, *supra* note 82, at 199–200.

[86] Waldman, *Cognitive Biases, supra* note 84, at 106 ("Framing concerns the way in which an opportunity is presented to consumers—namely, either as a good thing or a bad thing . . . is why technology companies explain their data use practices with leading language: 'if you don't allow cookies, website functionality will be diminished' or 'opting in to data collection will enable new and easier functionality.'").

[87] *Id.* at 108; WALDMAN, *supra* note 82, at 7.

[88] *See* HARTZOG, PRIVACY'S BLUEPRINT, *supra* note 82, at 142; Gregory Conti & Edward Sobiesk, *Malicious Interface Design: Exploiting the User*, ACM 271, 272 (2010) (identifying at least eleven techniques of malicious design: (1) Coercion—threatening or mandating the user's compliance; (2) Confusion—asking the user questions or providing information that they do not understand; (3) Distraction—attracting the user's attention away from their current task by exploiting perception, particularly pretensive processing; (4) Exploiting Errors—taking advantage of user errors to facilitate the interface designer's goals; (5) Forced Work—deliberately increasing work for the user; (6) Interruption—interrupting the user's task flow; (7) Manipulating Navigation—creating information architectures and navigation mechanisms that guide the user toward interface designer task accomplishment; (8) Obfuscation—hiding desired information and interface elements; (9) Restricting Functionality—limiting or omitting controls that would facilitate user task accomplishment; (10) Shock—presenting disturbing content to the user; (11) Trick—misleading the user or other attempts at deception); *see also* Luguri & Strahilevitz, *supra* note 85, at 53 (using another taxonomy of undue strategies to get consumers' consent in general—not only regarding information collection—which includes: (1) nagging—repeated requests to do something; (2) social proof—misleading statements about other consumers actions; (3) obstruction—asymmetry between signing up and cancelling; (4) sneaking products into baskets or hidden costs; (5) interface interference – obscuring important information; (6) scarcity— Consumer informed of limited quantities (7) forced action—tricking consumers to register; (8) urgency—misleading consumers regarding demand for the product).

privacy policy of a platform difficult to find or make it difficult to change the user's privacy settings.[89]

The term "privacy policy" itself confuses users by leading them to believe that if there is a "privacy policy," their information is safe.[90] However, in many cases these policies allow the collection of user information almost without limitations.[91] For example, Philips Sonicare electric toothbrush states that "the personal data we collect may include your first name, username, profile picture, email address, gender, birthday/age, country, language and password." And adds that "Philips may also work with third parties who process your personal data for their own purposes."[92]

Even if the design is not abusive, users' consent should be taken with a grain of salt. There are numerous ways for data to be collected, and granting multiple choices in their privacy settings can confuse the user on a topic they probably do not understand fully.[93]

---

[89] *See, e.g.*, Posner & Kenneally, *supra* note 70, at 10 (explaining that IoT devices often lack screens, so consumers cannot easily change privacy settings or access details about what data they are sharing).

[90] Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 19–20 (2021) ("In a typical finding, 75% of people incorrectly believed that the when 'a website has a privacy policy, it means the site will not share [their] information with other websites or companies.'").

[91] Waldman, *Cognitive Biases, supra* note 84, at 108 ("Websites cue trust through professional design while hiding their invasive data collection practices in inscrutable privacy policies"); Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 977 (2017) ("Privacy policies become 'anti-privacy policies' because companies know that we will never read them. The default settings for privacy controls are permissive, because companies know that we do not usually change them."); Christopher W. Savage, *Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy*, 22 STAN. TECH. L. REV. 95, 108 (2019) ("Privacy policies are written in a way that obscures what actually happens with the information gathered. As a result, people may understand in general terms that what they are buying is access to a website or social media service, but they have no real idea what it is that they are selling.")

[92] Jennifer Schlesinger, Andrea Day, *Most People Just Click and Accept Privacy Policies Without Reading Them—You Might Be Surprised at What They Allow Companies to Do*, CNBC (Mar. 15, 2019), https://www.cnbc.com/2019/02/07/privacy-policies-give-companies-lots-of-room-to-collect-share-data.html [https://perma.cc/Q9V8-KZJN].

[93] *See* Benjamin Scheibehenne et al., *Can There Ever Be Too Many Options? A Meta-Analytic Review of Choice Overload*, 37 J. CONSUMER RSCH. 409, 410 (2010) (reviewing literature on choice overload); *see also* ZUBOFF *supra* note 4, at 481–83; Posner & Kenneally, *supra* note 70, at 16 (proposing "just-in-time notifications" on data collection

A reasonable reading of all privacy policies that one encounters in a year requires seventy-six full workdays.[94] Thus, Users just click "I agree" and accept this reality as inevitable.[95] As such, their right to make their own decisions vanishes before they knew that there was a decision to be made.[96] Notice-and-choice models of privacy are thus most inadequate under precisely the conditions that define surveillance capitalism.[97]

Even if individuals invest their time in reading, they are not likely to understand the complex language,[98] grasp the complexity of what happens to data behind the screen or assess privacy risks in a meaningful way.[99] Rarely would users be made aware of how Big Data is analyzed, and how companies infer information from the data that users share.[100] Even if individuals understand a given privacy policy, in many cases they have no choice but to consent, because there is no equivalent alternative to the service.[101]

---

and sharing. Indeed, there are ways to improve users' awareness of data collection. Yet, there are so many data points and too many notifications might be perceived as a nuisance.).

94 *See* Alexis Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, ATLANTIC: TECH (Mar. 1, 2012) (summarizing a study by two Carnegie Mellon Professors, Lorrie Cranor and Aleecia McDonald, on the average time required for reading privacy policies).

95 *See* Turow, *Marketplace Privacy, supra* note 16, at 165; Solove, *The Myth of the Privacy Paradox*, *supra* note 99, at 5 ("Resignation is a rational response to the impossibility of privacy self-management."); s*ee also* RICHARDS, WHY PRIVACY MATTERS, *supra* note 20, at 92–108 (explaining that the concept of "privacy as control" and of consent that allows control is overwhelming, illusionary, insufficient and in fact a trap).

96 ZUBOFF, *supra* note 4, at 94.

97 *See* Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. 11, 17 (2020).

98 *See* OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 55–118 (2014); CASS R. SUNSTEIN, TOO MUCH INFORMATION, UNDERSTANDING WHAT YOU DON'T WANT TO KNOW 79–80 (2020); Florencia Marotta-Wurgler, *Even More Than You Wanted to Know About the Failure of Disclosure* 11 JERUSALEM. REV. LEGAL STUD. 63, 64 (2015); Uri Benoliel & Shmuel I. Becher, *The Duty to Read the Unreadable* 60 B.C. L. REV. 2255, 2277 (2019).

99 *See* Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 19 (2021).

100 *See* COHEN, *supra* note 65, at 56, ("'Big Data,' was a fast-evolving group of techniques for converting voluminous, heterogeneous flows of physical, transactional, and behavioral information about people."); Turow, *Marketplace Privacy, supra* note 16, at 160.

101 *See* VELIZ, *supra* note 3, at 14 (explaining that during COVID-19 lockdowns individuals were in fact forced to agree the terms of service of Zoom, to work and to allow

The value of consent and how it is received will probably be tested in courts in the future. However, for now, consent is usually legally valid when a consumer was given a mere "notice and choice,"[102] even without using reflective thinking.[103]

B. Data Analysis and Profiling

Analysis is the second stage of the data lifecycle. Companies strive to translate raw data into behavioral insights on users, using new technologies that are tools for engineering humanity.[104] Big Data, which is part of this effort, is based on the following: volume (the amount of data), velocity (the rate at which data is generated) and variety (the types of data collected).[105] Ubiquitous data collection from a variety of sources allows for interconnecting, analyzing, identifying, and extracting new and unpredictable value from data.[106] Complex algorithms mine the information from connected devices, find connections and correlations between data items, draw conclusions on individuals, and even predict their future behavior.[107]

Artificial Intelligence allows information processing that attempts to emulate human cognition by using computation power,

---

their children to attend distant learning. In fact, the service became indispensable, to be full participants in society).

[102] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (Mar. 2012); *see generally* Richards & Hartzog, *supra* note 82 (discussing the problems with consent).

[103] On automation of consent, see FRISCHMANN & SELINGER, *supra* note 28, at 60.

[104] *See* ZUBOFF, *supra* note 4, at 8 ("Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data.").

[105] *See* Daniel L. Rubinfeld & Michal S. Gal, *Access Barriers to Big Data*, 59 ARIZ. L. REV. 346 (2017) ("While big-data markets may differ substantially from one another, most big data sets share four main characteristics which contribute to their value: volume, velocity, variety, and veracity.").

[106] *See* Max N. Helveston, *Consumer Protection in the Age of Big Data*, 93 WASH. U. L. REV. 859, 867 (2016); Fred H. Cate & Viktor Mayer-Schönberger, *Notice and Consent in a World of Big Data, 3* INT'L DATA PRIV. L. 67, 69 (2013).

[107] *See* VIKTOR MAYER-SCHÖNBERGER & THOMAS RAMGE, REINVENTING CAPITALISM IN THE AGE OF BIG DATA 77–78 (2018); Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM L. REV. 1085, 1090 (2018) (explaining that algorithms "operate on the basis of correlation rather than 'causality' and produce 'predictions' rather than 'explanations'"); Lavi, *Targeting Exceptions, supra* note 61, at 95.

connectivity, and updatability.[108] Learning algorithms embedded in the system improve performance over time.[109] These algorithms are the engines behind data analytics.[110] The power of this technology grows exponentially as data expands.[111]

Technologies can also automatically integrate information and process patterns of individual behavior. An analysis of a Facebook user's "Likes" may allow the company to obtain an accurate evaluation of a wide range of personality traits of the user from her emotional state[112] to psychographic traits,[113] even if she never meant to share the information with anyone.[114] Companies can also draw conclusions on health information based on the language people use on social media.[115]

Driven by the need to increase users interaction, many businesses belonging to different industries are entering the metaverse nowadays.[116] As the metaverse develops "biometric monitoring

---

[108] *See* Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, U.C. DAVIS L. REV. 1, 54 (2017) ("AI is best understood as a set of techniques aimed at approximating some aspect of human or animal cognition using machines."); YUVAL NOAH HARARI, LESSONS FOR THE 21ST CENTURY 21–22 (2018) (explaining that AI possesses two particular non-human abilities: connectivity and updatability).

[109] *See* Calo, *supra* note 108, at 4–5.

[110] Manheim & Kaplan, *supra* note 43, at 120.

[111] *See* LANIER, TEN ARGUMENTS, *supra* note 30, at 6 ("The algorithms don't really understand you, but there is power in numbers, especially in large numbers.").

[112] *See* Michal Kosinski et al., *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*, 110 PROC. NAT'L ACAD. SCI. 5802–05 (Apr. 9, 2013); Wu Youyou et al., *Computer-Based Personality Judgments Are More Accurate Than Those Made by Humans,* 112 PROC. NAT'L ACAD. SCI. 1036–40 (Jan. 27, 2015).

[113] Psychographic profiles were at the core of the Cambridge Analytica Scandal. *See* Hannes Grassegger & Mikael Krogerus, *The Data That Turned the World Upside Down*, VICE (Jan. 28, 2017, 9:15 AM), https://www.vice.com/en/article/mg9vvn/how-our-likes-helped-trump-win [https://perma.cc/Q6HZ-E3WD]; *see also* Terrell McSweeny, *Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is the FTC Keeping Pace?* 2 GEO. L. TECH. REV. 514, 529 (2018); VAIDHYANATHAN, *supra* note 14, at 150–54.

[114] *See* ZUBOFF, *supra* note 4, at 274–77; Gregory Park et al., *Automatic Personality Assessment Through Social Media Language,* 108 J. PERSONALITY SOC. PSYCH., 934–52 (2015).

[115] *See generally* Raina M. Merchant et al., *Evaluating the Predictability of Medical Conditions from Social Media Posts,* 14 PUB. LIBR. SCI. ONE (2019).

[116] This revolution has already started: On October 28, 2021 Mark Zuckerberg, CEO of Facebook, published a founder letter and shared his vision stating that "[t]he next platform will be even more immersive—an embodied internet where you're in the experience, not just looking at it. We call this the metaverse, and it will touch every product we build" and

devices that are (or may soon be) incorporated into VR technologies can be used to make ads more persuasive—and manipulative."[117] They may also enable the development of biometric psychographic profiles, revealing consumers' involuntary psychological reactions to external stimuli, such as products or messaging.[118] The more data intermediaries collect, the better their predictive algorithms, the more powerful their ability to influence end users, and the better their ability to corner the market on digital advertising.[119]

Companies automatically capture every level of intimacy because technologies can measure reactions of users and the signals they create in real time and expand online surveillance into the real world. For example, Amazon's Just Walk Out ("JWO") technology uses Internet of Things ("IoT") technology "to allow cameras to capture every move of the customer in the Amazon Go store and directly charge their Amazon account afterwards."[120] Furthermore, wearable technology can present relevant content to shoppers while they are considering a product—say, in a grocery store, recognizing items a consumer has placed in the grocery cart and serving up relevant recipes through augmented reality. Brands could even tap body cues to tailor messaging. Sensor revealing that you're thirsty? Here's a coupon for smart water."[121] Applications can record users' reactions to advertisements, which help predict an advertisement's influence on sales.[122] Neuroimaging technology can even show

---

that "[his] hope is that within the next decade, the metaverse will reach a billion people, host hundreds of billions of dollars of digital commerce, and support jobs for millions of creators and developers." *See* MARK ZUCKERBERG, FOUNDERS LETTER, META (Oct. 28, 2021), https://about.fb.com/news/2021/10/founders-letter/ [https://perma.cc/6359-EUCR]; *see also eBay Steps into The Metaverse And NFTs With Trademark Application Filings*, TRADEMARKMALDIVES (Jul. 1, 2022) https://www.trademarkmaldives.com/blog/ebay-steps-into-the-metaverse-and-nfts-with-trademark-application-filings/ [https://perma.cc/8LZG-ELSZ].

117 Bloomberg, *supra* note 39.

118 *Id.*

119 *See* Jack M. Balkin, *How to Regulate (and Not Regulate) Social Media*, 1 J. FREE SPEECH L. 71, 84 (2021).

120 *See* Matene Alikhani, Bruno Renzetti, *Smile! You're on Camera: Data Collection in Food Retailing Markets*, YALE L. & POL'Y REV. (forthcoming).

121 See TUROW: THE AISLES, *supra* note 24, at 226.

122 *See* ZUBOFF *supra* note 4, at 281–84; Vincent Flood, *RealEyes are Able to Predict the Correlation Between Emotional Impact and Sales*, VIDEO AD NEWS (May 6, 2016), https://videoweek.com/2016/05/06/realeyes-are-able-to-predict-the-correlation-between-

whether various parts of the brain are engaged and whether a user will make a purchase before he makes a decision.[123]

Data processing and profiling offers predictions regarding users' future feelings and thoughts.[124] Thus, processing allows both feedbacks, but also feed-forward on behavior.[125] Companies can trade their predictions in a market, enrich the base of knowledge of other companies, improve predictions,[126] and increase profits.[127] While behavioral information was previously used primarily for the consumer's benefit, it is now used to predict and increasingly influence consumers to benefit the company.[128]

C. Influencing Decision Making and Behavior

> *Through manipulation of information you can . . . distort their realities until they cannot tell what is true any more.*[129]

Knowledge of individuals' behavior helps shape it. Influencing decision-making is the third stage of the lifecycle of data. Digital companies can make us act and think differently from the way we would in the absence of their influence.[130] By collecting and processing data, advertisers and other stakeholders can accurately target

---

emotional-impact-and-sales/ [https://perma.cc/74JR-WGAF] (describing how RealEyes, an emotional measurement company, has started to look at the correlation between how we feel during an ad, and how it affects our purchasing intent).

123 *See* Berman, *Manipulative Marketing*, *supra* note 45, at 520.

124 ZUBOFF, *supra* note 4, at 9, 95 (referring to data on the behavior of technology users as behavioral surplus).

125 HARCOURT, *supra* note 62, at 145–46.

126 ZUBOFF, *supra* note 4, at 10; Turow, *Marketplace Privacy*, *supra* note 16 ("[T]he Acxiom executive contended his firm can predict individuals' future behaviors because it knows demographic information about them, has actual offline and online purchase data about them . . . and can follow what they do on different digital devices.").

127 ZUBOFF, *supra* note 4, at 212 (explaining that market predictions allow certainty for profits).

128 Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. L. REV. 961, 972 (2021)

129 VELIZ, *supra* note 3, at 77.

130 RICHARDS, *supra* note 20, at 42; *see also* SINAN ARAL, THE HYPE MACHINE: HOW SOCIAL MEDIA DISRUPTS OUR ELECTIONS, OUR ECONOMY, AND OUR HEALTH—AND HOW WE MUST ADAPT 133 (2020) ("[S]ocial media advertising ecosystem is a persuasion market. Brands, governments and political campaigns invest in it to persuade us to change our behavior, from how we vote to what products we buy.").

messages to a susceptible audience.[131] New techniques for marketing are different from traditional ones,[132] since these techniques shift from general behavioral insights to personalized insights. The digital age allows extraordinary targeting and tailoring capabilities that are much stronger than ever witnessed before.[133]

1. From Behavioral Insights to Personalized Experiences

Traditional marketing models make use of behavioral insights, normally based on the general public's bounded rationality and vulnerabilities,[134] to influence consumers. For example, companies may predict an individual's behavior, influence the context, and nudge their consumers in transparent or non-transparent ways.[135] Since people tend to stick with the status quo when using default options,[136] companies try to set default rules and thereby influence users' behavior in their preferred ways.[137]

While previous models of influence were based on exploiting *general* insights, heuristics, and biases, the new data-driven models do not settle for mere exploitation of collective cognitive limitations of consumers. Instead, they build on personalization that is derived from ever-richer sources of behavioral data.[138] Surveillance

---

131 Tsesis, *supra* note 13, at 1590.

132 *See* Cohen*, supra* note 29, at 1; *see also* Ido Kilovaty, *Legally Cognizable Manipulation*, 34 BERKELEY TECH. L.J. 449, 475 (2019) (expanding on the exceptional nature of data manipulation).

133 Rauch, *supra* note 60, at 435.

134 On the problem of bounded rationality, see Daniel Kahneman, *Maps of Bounded Rationality: Psychology for Behavioral Economics,* 93 AM. ECON. REV. 1449, 1449 (2003) (explaining that when individuals make decisions, their rationality is limited by systematic biases that separate the choices they make from the optimal beliefs and choices assumed in economic rational-agent models); *see generally* Herbert A. Simon, *A Behavioral Model of Rational Choice*, 69 Q.J. ECON. 99 (1955).

135 A nudge is "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives." RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 6 (2008).

136 This systemic bias limits rationality. *Id.* at 8.

137 *See, e.g.*, Karen Levy & Solon Barocas, *Designing Against Discrimination in Online Markets*, 32 BERKELEY TECH. L.J. 1183, 1183, 1189, 1192 (2017) (analyzing how platform design and policy choices introduce opportunities for users' biases to affect how they treat one another).

138 ZUBOFF, *supra* note 4, at 279.

capitalism aims to exploit the unique biases of every *specific* person, provide him with personalized experiences, and deliver the most relevant content to the target.[139] It shapes a person's desires using complex means of behavior modification that fit the specific individual.[140] Companies tune behavior using subliminal cues designed to shape behavior at the precise time and place for maximum influence.[141] This method not only exploits existing biases but creates new ones by manipulating a variety of pressure points.[142]

2. Finding the Susceptible Consumer and Targeting Vulnerabilities

> *Reach millions of US consumers based on real world behaviors and inspire them in the moments that matter – while they're making purchase decisions.*[143]

Data is power. When companies have access to private information, they may influence the actions of the subject who produced it. New technological tools allow companies to design every aspect of the interaction with the consumer and exploit his biases.[144] Today, companies may choose which consumers they wish to approach and

---

[139] Facebook's "FBLearner Flow," which is based on machine learning, ingests trillions of data points every day and deploys them to the server fleet for live predictions. *See* ZUBOFF, *supra* note 4, at 279.

[140] *See generally* Karen Yeung, '*Hypernudge': Big Data as a Mode of Regulation by Design*, 20 INFO., COMMC'N., & SOC'Y. 118 (2017) (arguing that Big Data's extensive harvesting of personal digital data is troubling due to the particular way in which that data is being utilized to shape individual decision-making to serve the interests of commercial Big Data barons); Calo, *supra* note 108, at 18 ("[F]irms can manipulate other market participants through a fine-tuned understanding of the individual and collective cognitive limitations of consumers."). *See also* Calo, *supra* note 31, at 1007-09; HARCOURT, *supra* note 62, at 145–46; ZUBOFF *supra* note 4, at 18.

[141] ZUBOFF *supra* note 4, at 295 (explaining how to tune behavior).

[142] *See* Susser et al., *supra* note 32, at 28.

[143] This is the slogan of inMarket, which aims to connect brands and consumers at the right timing to sell to consumers and increase the likelihood of a purchase. *See* INMARKET, www.inmarket.com/ [https://perma.cc/EEJ6-LBFY]. The company specializes in geo-targeting advertising for the physical world. "Using real-time data from 50 million first-party integrations with the world's most popular apps, inMarket identifies and engages consumers at every stage of the shopping cycle and creates exciting experiences that drive huge campaign ROI for the world's top brands." *About Us*, INMARKET, inmarket.com/about/ [https://perma.cc/R27B-6643].

[144] Calo, *supra* note 31, at 1004; HARTZOG, *supra* note 82, at 202 ("Precision advertising can be used to exploit biases.").

when they wish to do so. They do not need to wait for the consumer to enter the shop; instead, they can contact the consumer.[145] Technology allows companies to know consumers' physical locations, their heart rates, and other biometric data.[146] Algorithms that process and update a consumers' information allow constant supervision and make it possible for corporations to adjust the manner in which a consumer is approached.[147] This is social engineering at its height.[148]

a) Targeting Consumers Based on Lifestyle Patterns and Location

Companies collect data on consumers online by tracking browsing activities, clicks, cookies, and actual purchases.[149] Visiting a website about depression? Advertisers, social media companies, and data brokers are likely tracking and targeting you, [150] both on-and-offline.[151] Companies gain insights on the lifestyle and location of specific consumers and map their interests and needs throughout the day.[152] Companies exploit this goldmine of knowledge and evaluate

---

145 HARTZOG, *supra* note 82, at 202 ("Precision advertising can be used to exploit biases.").

146 *See* ZUBOFF *supra* note 4, at 86, 95, 153.

147 *See* TUROW: THE AISLES, *supra* note 24, at 188–89 ("Based on what it knows about the group's purchasing habits in terms of products and the channels it uses for retail purchases (the Web, the phone, the store), the company will approach individual customers with particular messages and offers tuned to their group . . . . The key to successful personalization, he said, involves optimizing the use of the company's data management platform. It contains information about all the firm's identified purchasers, including "every single digital touch point.").

148 *See* FRISCHMANN & SELINGER, *supra* note 28, at 126.

149 *See* TUROW, *supra* note 19, at 34.

150 *See Your Mental Health for Sale,* PRIV. INT'L, https://privacyinternational.org/campaigns/your-mental-health-sale [https://perma.cc/U9LR-9B9Z].

151 *See* TUROW, *supra* note 24, at 127 (referring to inMarket, a commercial company that made deals with many retailers to place Bluetooth Low Energy (BLE) boxes with the inMarket code throughout their stores and to put inMarket codes in those retailers' apps, so that shoppers with the apps on their phones they could be pinged by the inMarket boxes as they moved through the stores).

152 ZUBOFF *supra* note 4, at 242–43; *see also* TUROW, *supra* note 24, at 107; Calo*, supra* note 31, at 1016.

whether specific individuals are "targets" or "waste" and send their ads to relevant consumers accordingly.[153]

For example, Wi-Fi and Bluetooth in consumers' smart devices can communicate with special systems that retailers install in their stores, allowing retailers to monitor potential consumers inside and outside the store, as well as attracting them into the store by sending potential consumers special offers.[154] Companies can buy Bluetooth Low Energy (BLE), which transmits a signal with a device ID that alerts an app on a smart device carried by a potential consumer when the person passes by an area.[155]

Companies lure consumers to install the retailers' app which maps their movements inside and outside the store.[156] In other cases, companies plant tracking apps that piggyback onto other apps.[157] For example, traffic-analytics firms piggyback onto other companies' apps to attract increasing numbers of clients.[158] The consumer

---

153 TUROW, *supra* note 19, at 88; ARAL, *supra* note 130, at 203 ("Platforms like Facebook, Twitter and YouTube provide connections, communication and content to get consumers' attention. They then sell that attention to brands, governments, and politicians who want to change people's perceptions, opinion and behaviors with ads.").

154 TUROW, *supra* note 24, at 116 (retailers aspire to make consumers spend more time in a store because there is a correlation between the amount of time shoppers spend in a store and the amount of money they spend). This is also true of online influence, which aims to lure consumers to spend more time on the website. *See* TUROW, *supra* note 19, at 188–91.

155 TUROW, *supra* note 24, at 120–21("Companies can buy inexpensive BLE boxes, which act as beacons, transmitting a signal with a device ID. If a phone app within that range is compatible with that ID, the signal alerts the app to send a message via cellular or Wi- Fi that the phone has made a connection with the BLE beacon in a particular location. With an array of its BLE beacons tuned to its app in a retail location, the app owner can therefore figure out the movement of the phone's holder as she or he moves through the store.")

156 *See* TUROW, *supra* note 24, at 120–21.

157 *Id.* at 128 (describing how inMarket gains information on a variety of consumers without obtaining their explicit permission); *see also* Michalis Diamantaris et. al., *This Sneaky Piggy Went to the Android Ad Market: Misusing Mobile Sensors for Stealthy Data Exfiltration*, CCS '21, November 15–19, 1065 (2021) ("[A]s in-app ads can 'piggyback' on the permissions intended for the app's core functionality, they can also obtain information from protected sensors such as the camera, microphone and GPS."); Gabriel Nicholas & Aaron Shapiro, *Failed Hybrids: The Death and Life of Bluetooth Proximity Marketing*, 9 MOBILE MEDIA & COMMC'N 465, 477 (2021) ("Google's apps meant that the tech giants could passively engage in Skyhook-style 'wardriving' to map Bluetooth signal in the wild by piggybacking off ambient broadcasts from non-beacon Bluetooth devices, such as smartphone payment systems, security cameras, or speakers.").

158 *See* TUROW, *supra* note 24, at 123.

is not aware that an app is constantly spying on his location, and pushing targeted advertisements, offers, personalized ads, and discounts onto his device accordingly,[159] as he approaches specific products.[160]

Supermarket coupon dispensers can target personalized offers to a consumer based on his historical purchases, brand preferences and loyalty, his location in the store, and the items he already took to the shopping cart.[161] Companies started extending their reach outside the physical store via GPS and Waze.[162] These apps target coupons to a potential consumer, who drives near a store and directs him to the store when he clicks on the coupon.[163] Navigation apps can collect and process information on many consumers and improve the precision and timing of targeting.[164]

---

159 *Id.* at 123–24.

160 *Id.* at 126–27.

161 *Id* at 132 (describing supermarket and drugstore coupon dispenser Catalina Marketing).

162 TUROW, *supra* note 24, at 135 ("Given the exhaustive efforts to target people's mobile devices inside brick- and- mortar establishments, it is not surprising that this technology began to extend outside the physical store. Facilitating this development was a GPS (global positioning system) chip that, by the 2010s, manufacturers were installing in every smartphone. The chip picks up the beaconlike signal of three geostationary satellites; software in the phone triangulates the data into map coordinates.").

163 TUROW, *supra* note 2424 at 135–36 ("The highest-quality commercial GPS receivers can pinpoint someone's position to better than 11.5 feet, and when combined with the location of Wi- Fi pings from stores and other places, the location can be even more precise. Consequently, if a smartphone owner allowed an email provider, an app, or a website to access the phone's location, that information could be used to sell ads to merchants near that phone.")

164 TUROW, *supra* note 24, at 136–38. Companies develop special interfaces to make it easier for advertisers to collect more data on users and refine their advertisements and the potential target audience. *See* Daniel Kreiss & Matt Perault, *Four Ways to Fix Social Media's Political Ads Problem—Without Banning Them*, N.Y. TIMES (Nov. 2, 2019), nytimes.com/2019/11/16/opinion/twitter-facebook-political-ads.html [https://perma.cc/393F-3PS2] ("Facebook allows advertisers to bring their own data to their platforms for targeting purposes, and Twitter has similar tools for commercial ads."); *see also* Christina Newberry*, How to Set Up Meta Pixel (Formerly Facebook Pixel),* HOOTSUITE (Feb. 18, 2022), https://blog.hootsuite.com/facebook-pixel/ [https://perma.cc/374S-GE4A]; *Twitter Ads Targeting*, TWITTER BUS., business.twitter.com/en/targeting.html [https://perma.cc/Q5RF-DJPL]; Pauline T. Kim, *Manipulating Opportunity,* 106 VA. L. REV. 867, 876 (2020).

b) Targeting Consumers Based on Personality Traits

The location of a potential consumer does not necessarily predict his opinions and preferences. To this end, advertisers turn to psychographic profiling, a technique that creates a personality profile of an individual based on the following five personality traits:[165] Openness (the need for new experiences); Conscientiousness (whether a person prefers the status quo or needs changes); Extroversion (whether a person is friendly), Agreeableness (whether a person takes care of others and puts their needs before his); and Neuroticism (whether a person tends to worry).[166] Psychographic characteristics can be deduced from personality questionnaires[167] or predicted from the digital fingerprints of individuals in the form of likes on Facebook and Tweets.[168] For example, Cambridge-Analytica developed the model for predicting behavior of voters and targeting political messages,[169] but the company's method can also be used for commercial purposes.[170] Such profiles can improve the persuasive power of commercial messages.[171]

c) Targeting Consumers Based on their Current Mood and Emotional State

The methods of surveillance online and offline allow companies to know consumers' moods and emotional state. Companies gather psychological insights and use the data to pinpoint the exact moment at which a person needs a "confidence boost" and is most vulnerable

---

165 *See* ARAL, *supra* note 130, at 206 (explaining that microtargeting models are powered by reams of personal data about consumers' demographics, behaviors, preferences, and psychological profiles); Kilovaty, *supra* note 132, at 465.

166 The five characteristics are known as the OCEAN model (a notarikon of the personality traits). Hannes Grassegger & Mikael Krogerus, *The Data That Turned the World Upside Down,* VICE: MOTHERBOARD (Jan. 28, 2017, 9:15 AM), https://www.vice.com/en/article/mg9vvn/how-our-likes-helped-trump-win [https://perma.cc/SQ8L-Y8QQ]; *see also* VAIDHYANATHAN, *supra* note 13, at 151 (explaining that psychographic profiles make it possible to understand a persons' personality even when they are outside the group they belong to).

167 *See* Cadwalladr & Graham-Harrison*, supra* note 10.

168 VAIDHYANATHAN, *supra* note 14, at 154.

169 *Id.* at 155.

170 *See generally* Sandra C. Matz et al., *Psychological Targeting as an Effective Approach to Digital Mass Persuasion*, 114 PROC. NAT'L ACAD. SCI. U.S. 12714 (2017).

171 ARAL, *supra* note 130, at 216.

to a specific product. They monitor every interaction of their potential consumer and figure out the exact moment in which the consumer feels "stressed," "defeated," "overwhelmed," "anxious," "nervous," etc.[172]

Additionally, social media giants in general, and Facebook in particular, conduct various experiments involving use of linguistic analysis to detect users' emotional states.[173] Their aim is to learn to discern activities, interests, moods, appearances, and more.[174] Beyond analysis of text, there are facial recognition systems combined with learning algorithms that can automatically identify people appearing in users' digital photo albums and tag them.[175] Knowing who a person is allows for better targeting. This technology makes it possible to identify emotions in videos and images and improve messaging. The result is more accurate targeting.[176] For instance, Facebook developed a video- and image-understanding platform called Lumos, a tool that can comb through photos or videos uploaded to Facebook, Instagram, and other platforms and learn what

---

[172] ZUBOFF *supra* note 4, at 305; Whigham, *supra* note 32 ("[*T*]*he Australian* obtained internal documents from the social media giant which reportedly show how Facebook can exploit the moods and insecurities of teenagers using the platform for the potential benefit of advertisers. The confidential document dated this year detailed how by monitoring posts, comments and interactions on the site, Facebook can figure out when people as young as 14 feel 'defeated,' 'overwhelmed,' 'stressed,' 'anxious,' 'nervous,' 'stupid,' 'silly,' 'useless,' and a 'failure.' Such information gathered through a system dubbed sentiment analysis could be used by advertisers to target young Facebook users when they are potentially more vulnerable.").

[173] Cohen*, The Emergent Limbic Media*, *supra* note 29.

[174] *See* Aviva Rutkin, *Facebook Can Recognize You in Photos even If You're Not Looking,* NEW SCIENTIST (June 22, 2015), https://www.newscientist.com/article/dn27761-facebook-can-recognise-you-in-photos-even-if-youre-not-looking/ [https://perma.cc/2PU5-FMSB].

[175] It should be noted that Facebook (Meta) had such a system and announced it was shutting it down. *See* Kashmir Hill, Ryan Mac, N.Y TIMES (Nov. 2, 2021) https://www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.html.

[176] Yasin Altaf, *Your Face is the Future of Targeted Marketing. Here's Why Businesses Should Use Facial Recognition*, ENTREPRENEUR (Oct. 14, 2022) https://www.entrepreneur.com/science-technology/facial-recognition-the-future-of-targeted-marketing/437103 ("With the ability to scan faces and determine key attributes like age and emotions, face recognition technology empowers businesses with essential consumer data that can target product promotions and subsequently improve product offerings.")

they contain.[177] It pushes images to the next stage: understanding images at the pixel level. It "conducts sophisticated facial recognition to uniquely identify people and emotions in their facial expressions,"[178] Such a system can help identify a user's likes and habits on the basis of photos in a user's feed.[179]

Such systems allow media giants and other companies to influence viewers in the most effective way: by serving ads calibrated to certain emotions.[180] Companies also use facial recognition technology[181] to decode the emotional state of consumers offline by using data from smart devices[182] and cameras in shopping centers.[183] Several companies, such as Face-Six and Cameralyze,[184] already offer retailers the ability to use facial recognition technology and detect the current emotions of the people walking through their aisles.[185]

---

177 Scott Berinato, *Inside Facebook's AI Workshop*, HARV. BUS. REV. (July 19, 2017), https://hbr.org/2017/07/inside-facebooks-ai-workshop.

178 ARAL, *supra* note 130, at 79–80.

179 Berinato, *supra* note 177.

180 Sandra C Maltz et.al., *Psychological Targeting as an Effective Approach to Digital Mass Persuasion*,114 PROC. NAT'L ACAD. SCI. 12714, 12717 (2017) ("mood could indicate a critical time period for psychological persuasion").

181 *See* KATE CRAWFORD: Atlas of AI AI154 (2021); ZUBOFF *supra* note 4, at 252–55; Yaniv Taigman et. al., *Deep Face: Closing the Gap to Human-Level Performance in Face Verification,* FACEBOOK RSCH. (Apr. 14, 2018) (detailing the 2018 announcement that a Facebook research team is able to recognize faces); Annie Lin, *Facial Recognition Is Tracking Customers as They Shop in Stores*, *Tech Company Says*, CNBC (Nov. 23, 2017), https://www.cnbc.com/2017/11/23/facial-recognition-is-tracking-customers-as-they-shop-in-stores-tech-company-says.html [https://perma.cc/34Y9-X2YY].

182 *See* Spencer, *supra* note 33, at 979 ("[W]eb results based on the user's 'current emotional state,' based on indicia of mood drawn from webcam facial recognition, a scan of the user's heart rate, and even the "user's brain waves"); Sidney Fussell, *Alexa Wants to Know How You're Feeling Today*, ATLANTIC (Oct. 12, 2018), https://www.theatlantichttps://www.theatlantic.com/technology/archive/2018/10/alexa-emotion-detection-ai-surveillance/572884/ [https://perma.cc/9LTS-E6M5].

183 TUROW, *supra* note 24, at 123 ("Raul Verano, chief technology officer for the analytics firm Shopperception, said that his company had installed cameras with 3D sensors in stores to track shopper activity in proximity to goods made by the company's clients. ")

184 TUROW, *supra* note 24, at 228; *see, e.g.*, CAMERALYZE, https://www.cameralyze.co/facial-emotion-recognition-with-artificial-intelligence (Jan. 9, 2023) ("Cameralyze offers the most accurate and automated system for identifying human emotions from facial expressions . . . .")

185 Lauren E. Knudson, *Stalking in the Grocery Aisles: Using Section 5 of the FTC Act to Curtail Big Data Driven Price Discrimination*, 107 IOWA L. REV. 1283,1289 (2022) ("In addition, FRT can collect more detailed information. Some FRT companies claim to 'offer

They sort the movements by emotional categories, such as anger, disgust, joy, surprise, or boredom.[186] Consequently, companies make powerful ads targeting and influencing consumers in vulnerable emotional states.[187]

d) Targeting Consumers Based on Their Online Engagement and Social Relations

Companies optimize content to consumers based on their engagement.[188] They can draw conclusions on consumers based on their clicks on content and ads, "Likes," and "Shares," and based on the topics they discuss with their friends on social networks, creating a feedback effect.[189] But this does not present the whole picture. Relationships between users of social networks allow companies to

---

retailers the ability to detect the current emotions of the people walking through their aisles.'"); Kiely Kuligowski, *Facial Recognition Advertising*, BUS. NEWS DAILY (Oct. 20, 2022), https://www.businessnewsdaily.com/15213-walgreens-facial-recognition.html ("[T]he sensors and cameras in the refrigerator doors connect to face-detection technology that can identify a customer's age and gender. They can also glean external factors, like if it's hot or raining outside and how long the person has been standing there, and even pick up on the person's emotional response to what they're looking at.").

186 TUROW, THE AISLES, *supra* note 24, at 228.

187 *See* Louise Matsakis, *Facebooks' Targeted Ads Are More Complex Than It Lets On*, WIRED (Apr. 25, 2018), https://www.wired.com/story/facebooks-targeted-ads-are-more-complex-than-it-lets-on/ [https://perma.cc/W2AC-MCRP]; Sam Levine, *Facebook Told Advertisers It Can Identify Teens Feeling 'Insecure' and 'Worthless,'* GUARDIAN (May 1, 2018) https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens [https://perma.cc/E5A6-R373]; Cohen*, supra* note 29, at 9 ("Facebook acknowledged having served different advertisements to teenaged girls and young women based on considerations such as detected levels of depression and dissatisfaction with self-image.").

188 Cohen*, The Emergent Limbic Media*, *supra* note 29, at 9.

189 TUROW, THE AISLES, *supra* note 24, at 154; *see also* Rebecca J. Rosen*, Armed with Facebook 'Likes' Alone, Researchers Can Tell Your Race, Gender, and Sexual Orientation*, ATLANTIC (Mar. 12, 2013), https://www.theatlantic.com/technology/archive/2013/03/armed-with-facebook-likes-alone-researchers-can-tell-your-race-gender-and-sexual-orientation/273963/ [https://perma.cc/64WB-AV5P]; James P. Bagrow et al., *Information Flow Reveals Prediction Limits in Online Social Activity*, 3 NATURE HUM. BEHAV. 122 (2019); COHEN, BETWEEN TRUTH AND POWER, *supra* note 65, at 85 ("[S]ocial networking as Facebook and microblogging platforms such as Twitter function as de facto aggregators for a wide range of content and deliver feeds optimized to everything that is known or inferred about particular users' opinions and beliefs. By design, all of those algorithms incorporate feedback effects, and so their operation both reflects and continually reinforces the powerful economic motivation to peruse viral spread.").

characterize consumers, assigning them a "social influence score."[190] As the saying goes, "tell me who your friends are and I will tell you who you are."[191] Because many apps including fitness and health tracking apps encourage users to register with their social network log-ins, instead of creating an account,[192] information on their social connections spills beyond the social media platform.[193] This allows app owners to target consumers *and their friends* online and offline. They can encourage consumers to publicize their store on social networks, promote their brands, and offer them discounts based on the number of friends they have and their potential influence.[194]

3. How to Influence? New Tools and Strategies of Manipulative Influence

Targeting susceptible users is only part of the story. Companies employ strategies that do not necessarily consist of persuasion.[195] Instead, they *create a context of vulnerability* to push potential consumers to their products. Companies use cognitive psychology to

---

190 Edith Ramirez et al., *Federal Trade Commission, Data Brokers: A Call for Transparency and Accountability*, FED. TRADE COMM'N. (2014).

191 TUROW, THE DAILY YOU, *supra* note 19, at 138–40; Johan Ugander, *Monophily in Social Networks Introduces Similarity Among Friends-of-Friends*, 2 NATURE HUM. BEHAV. 284 (2018); Solon Barocas & Karen Levy*, Privacy Dependencies,* 95 WASH. L. REV 555 (2020).

192 *See* Paul Wright, *The Advantages and Disadvantages of Social Logins: What You Need to Know*, RC (Aug. 9, 2021) https://www.rubbercheese.com/insights/social-logins/.

193 *See* Talon Homer, *Should You Use Facebook or Google to Log In to Other Sites*?, HOWSTUFFWORKS (Apr. 13, 2022) https://computer.howstuffworks.com/internet/social-networking/networks/facebook-google-single-sign-on.htm; Andrei Kazlouski et. al., *Do Partner Apps Offer the Same Level of Privacy Protection? The Case of Wearable Applications,* 2021 IEEE International Conference on Pervasive Computing and Communications Workshops 648, 652 (2021) ("These apps allow user to register/sign in with their Facebook profile. It is natural to assume that in that case, the social network will be contacted. However, we established that Facebook is contacted, and the data are shared regardless of whether a user is registered in the social media or attempting to sign in with her Facebook credentials. Hence, the social network is able to gather data about customers beyond its userbase.")

194 TUROW, THE AISLES, *supra* note 24, at 5 ("The chain also bases its formulas for offering you discounts partly on an 'influence' score it has bought from a company that evaluates the number of friends you have on social media and your degree of influence on them.")

195 Cohen*, The Emergent Limbic Media*, *supra* note 29, at 9.

influence decisions in ways that do not reach the threshold of consciousness.[196] They target the intuitive, emotional, and instinctive mode of thought ("system 1"), while bypassing the deliberative mode of thought ("system 2").[197] To do so, they use dark patterns and non-informational marketing strategies that include promotional techniques that fall along a continuum relating to their visibility: there are apparent way of influence that "critical viewers can see the technique at work and at least attempt to resist its influence", on the other side of the continuum, there are "problematic forms of manipulative marketing operate almost entirely outside of consumers' conscious awareness."[198] They target emotions such as fear, love, patriotism, as well as treasured institutions like family and community,[199] and experience with individual reactions without receiving prior approval such as Institutional Review Board (IRB) for this experimentation.[200] Companies act as social actors and utilize

---

196 Berman, *Manipulative Marketing, supra* note 45, at 518 (referring to targeting the subconscious).

197 *See* DANIEL KAHNEMAN, THINKING, FAST AND SLOW 237 (2011) (explaining the two systems of thinking, or modes of thought: intuitive thinking ("system 1") and deliberative analytic thinking ("system 2")); *see also* Shmuel I. Becher & Yuval Feldman, *Manipulating, Fast and Slow: The Law of Non-Verbal Market Manipulations,* 38 CARDOZO L. REV. 459, 474–76 (2016) (defining non-verbal marketing manipulation).

198 Berman, *Manipulative Marketing, supra* note 45, at 517, 522 *(*"[M]arketers (1) are most successful when emotional content—not information—is presented to consumers, (2) can carefully craft marketing appeals (using humor and other non-informational techniques) to increase the viewer's/reader's receptivity to the marketing message while disengaging critical faculties, and (3) can influence consumer behavior without consumers being aware of the powerful effect of advertising."); Becher & Feldman, *supra* note 197 (referring to non-verbal market manipulation, such as the colors of shopping sites and music in shopping centers); Tamara Piety, *Advertising as Experimentation on Human Subjects,* 19 ADVERT. & SOC'Y Q. 22 (2018) ("Typically these efforts . . . take place beneath our level of awareness; so that the appeals which move us are often, in a sense, 'hidden.' The result is that many of us are being influenced and manipulated, far more than we realize, in patterns of our everyday lives.").

199 *See* Piety, *supra* note 198.

200 Berman, *Manipulative Marketing, supra* note 45, at 524 (referring to "sensory advertising" or "sensory branding," that is, "marketing that engages the consumers' senses and affects their perception, judgment and behavior"). Regarding the requirement for a prior review board approval for experimenting with human reactions in academic contexts, see Piety, *supra* note 198 ("The IRB process is supposed to ensure that research subjects' participation is voluntary and informed, and that the potential benefits of the research outweigh the potential harms. Yet there is no IRB for our present-day marketing environment.").

bots.[201] These software programs initiate communication and allow corporations to promote their brands online.[202] They can even provide false information and undermine the ability of consumers to make educated decisions. Companies also combine cognitive psychology with social psychology to change dynamics on social networks.[203] They do so by utilizing their algorithms to create a "framing effect,"[204] emphasizing specific information that users posted in newsfeeds of other users and reinforcing social pressures.[205] Arguably, social pressure is conscious, yet the initial opaque algorithmic targeting bypasses deliberative thinking.[206]

Neuroscience marketing at the service of companies allows them to measure users' response of users to influence, including effects of a brand on users' subconscious in real time and improve their

---

[201] *See* Madeline Lamo & Ryan Calo, *Regulating Bot Speech*, 66 UCLA L. REV. 988, 993 (2019) ("[B]ots are software programs that run according to instructions. We use the term here to refer to automated agents that initiate communication online, by phone, or through other technologically mediated means."); Luguri & Strahilevitz, *supra* note 85, at 44 ("Dark patterns are user interfaces whose designers knowingly confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions. They typically prompt users to rely on System 1 decision-making rather than more deliberate System 2 processes."); *see also* Cass R. Sunstein, *Manipulation As Theft* (July 4, 2021) (referring to manipulation of some "dark patterns" that "take something from someone for the benefit of another" as theft).

[202] Sunstein, *supra* note 201, at 6 (referring to commercial bots).

[203] *See* Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. 335, 335 (2014).

[204] *See* THALER & SUNSTEIN, *supra* note 135, at 36 (expanding on the "framing effect," under which choices depend, in part, on the way problems are stated).

[205] *See* Michal Lavi, *Publish, Share, Re-Tweet, and Repeat*, 54 U. MICH. J. L. REFORM 441, 461–62 (2021). ("[I]ntermediaries frequently 'utilize algorithms to prioritize newsfeed content created by a user's close friends and family, which reinforces existing biases and further encourages dissemination." (citation omitted)); Eduardo Hargreave et. al , *Biases in the Facebook News Feed: a Case Study on the Italian Elections*, International Conference on Advances in Social Networks Analysis and Mining 806, 812 (2018) ("We were able to conclude that the algorithm tends to reinforce the orientation indicated by users about the pages they 'like,' by filtering posts and creating biases among the set of followed publishers.").

[206] Regarding hidden reasons for influence and manipulation, see Daniel Susser et al., *Online Manipulation: Hidden Influences in a Digital World,* 4 GEO. L. TECH. REV. 1, 24 (2019) ("Hidden influences thwart such assumptions. If people learned after some time that the real reason graphic health warnings were placed on cigarette packages is that the alcohol lobby paid off government officials, in an attempt to drive people away from smoking and toward drinking, the influence would be hidden in the relevant sense and the public would rightly feel manipulated.").

targeting,[207] Currently, over a hundred companies offer their services for neuromarketing worldwide and marketing and media agencies utilize these services.[208] Companies experiment with influence, assess feedback, and select the most effective tool, without necessarily understanding why.[209] The following section focuses on central strategies of targeting. It should be noted that the strategies are not a closed list, and more tools of influence are likely to develop in the future.

a) Engineering Emotions, Stimulating Emotions and Targeting Senses

In 2014, Facebook's Core Data Science Team, along with academic researchers, manipulated the news feeds of randomly selected users by increasing either positive or negative content to see if this would create "emotional contagion."[210] They exposed one group to positive messages in their newsfeed, and the other group to predominantly negative messages to the other group. The idea was to test whether subliminal exposure to specific emotional content would cause people to change their own posts. It did. The tone of users' posts changed to reflect the respective newsfeed they had received.[211] This emotional engineering was part of an experiment; yet

---

[207] Berman, *Manipulative Marketing, supra* note 45, at 518 (explaining that neuromarketing specialists measure the brain's response to marketing stimuli in real time allowing companies to determine individuals' emotional responses to brands and brand preferences, even when the individual may be unaware of the brand's effect on his subconscious decision making); *see also* Cohen*, The Emergent Limbic Media*, *supra* note 29, at 68 (explaining the role of neuroscience in the departure from traditional persuasion).

[208] *See* Bernd Eberhart, *How Companies Are Using Neuromarketing to Influence What Brands You Buy*, BUS. STANDARD (Apr. 10, 2018) https://www.business-standard.com/article/companies/how-companies-are-using-neuromarketing-to-influence-what-brands-you-buy-118041000279_1.html.

[209] Zarsky, *Privacy and Manipulation, supra* note 24, at 170; Richards & Hartzog, *supra* note128, at 16*;* Nahid Sharif, *Top 5 Proven Neuromarketing Strategies Every Marketer Should Know About,* WEDEVS (Oct. 13, 2022) https://wedevs.com/blog/375567/neuromarketing-strategies-for-marketers/.

[210] *See generally* Kramer et al., *supra* note 36; James Grimmelmann, *The Law and Ethics of Experiments on Social Media Users*, 13 COLO. TECH. L.J. 219 (2015); *see also* FRISCHMANN & SELINGER, *supra* note 28, at 117–18 (describing Facebook's cognition experiment on user emotions). This experiment teaches us that surveillance gives the watcher the power to persuade and manipulate. *See* Richards, *supra* note 20, at 151.

[211] ZUBOFF, *supra* note 4, at 301.

it is not an anecdotal episode. Because companies know that a change in a users' mood affects his decision making,[212] they use strategies to affect users' mood and enhance emotional arousal.[213] Thus, companies often stimulate emotions, leading to emotional responses,[214] such as sadness or happiness,[215] fear,[216] anxiety,[217] or other emotions,[218] to enhance their profits.

Targeting the senses plays a role in stimulating consumers and affects their perception, judgment, and behavior.[219] In the past, this type of stimulation occurred mostly offline by the design of shops, colors, music, and scent, for example.[220] The IoT opens more possibilities of marketing that engages with consumers' senses and allows personalized stimulation that fits preferences of specific consumers.

b) Targeting by Utilizing Human-ish Artificial Intelligence Entities

More than a decade ago, studies identified the potential for advertisers to serve as social actors in persuading and influencing potential consumers.[221] Today, Artificial Intelligence agents operate

---

212 *See, e.g.*, FRISCHMANN & SELINGER, *supra* note 28, at 117–18 (describing Facebook's cognition experiment on user emotions). This experiment teaches us that surveillance gives the watcher the power to persuade and manipulate); *see* Richards, *supra* note 20, at 151

213 ARAL, *supra* note 130, at 167.

214 Piety, *supra* note 198 ("[M]arketers often rely on stimulating fear, anxiety, jealousy, lust, avarice, hunger, and insecurity; in short, a whole repertoire of emotions and desires.").

215 Becher & Feldman, *supra* note 197, at 483.

216 Piety, *supra* note 198 ("Advertising professionals readily admit that fear can sell products. Indeed, a great deal of research was directed at attempting to find the 'optimal' level of fear. As one textbook puts it, 'the appeal to fear is especially effective as a means of enhancing motivation.'").

217 *Id.* ("A good deal of the fear that advertising attempts to stimulate is perhaps more appropriately described as 'anxiety'—usually about conforming to social norms in dress, grooming, attractiveness, and weight.").

218 VAIDYANATHAN, *supra* note 14, at 5–6 (explaining that Facebook promotes items that stimulate emotional responses in order to promote engagement).

219 Berman*, supra* note 45, at 524.

220 Becher & Feldman, *supra* note 197, at 476–83 (giving examples of the colors inside the shops and the design and color of shop windows that affect the motivation to enter the shop and the time spent there, as well as the music in shops which affects the items consumers buy, and the scent in shops).

221 *See* B.J. FOGG, PERSUASIVE TECHNOLOGY, USING COMPUTERS TO CHANGE WHAT WE THINK AND DO 24–28, 287 (2003); Tsesis, *Marketplace of Ideas, supra* note 13, at 1621

on social media and as assistive technologies. They can mimic a real person over the phone[222] or via connected devices.[223] AI agents are designed to create a natural interaction experience between humans and algorithms and may trick consumers into assuming they are interacting with a human.[224] Such bots can influence the context of advertisements in different ways and persuade users by imitating human feedback and support. In the age of Metaverse, the capabilities to utilize human-ish features will be much more significant as "consumers will be targeted by simulated people, products, and activities that seem just as real as everything else around us."[225]

The fact that they behave similarly to humans, cues consumers' trust and makes them vulnerable to manipulation.[226] Individuals treat bots as humans, and these bots are designed to designed to solicit trust individuals ordinarily reserve for humans. As bots become more human*ish*, emotional responses to them are expected to grow stronger.[227]

c) False information and Fake Speakers

Companies may implant false beliefs held by their consumers, and undermine their assumptions, to induce them to buy a product

("[B]ots pose as humans on Facebook, Twitter, and other social media, and they transmit messages as directed including hundreds of millions of governmental and private-actor posts.").

222 *See, e.g.*, Yaniv Leviathan & Yossi Matias, *Google Duplex: An AI System for Accomplishing Real-World Tasks Over the Phone,* GOOGLE AI BLOG, (May 8, 2018), https://ai.googleblog.com/2018/05/duplex-ai-system-for-natural-conversation.html [https://perma.cc/HGU7-J357]. Google Duplex technology can conduct natural conversations in order to carry out specific tasks, such as scheduling appointments over the phone. By mimicking ordinary interaction, including the incorporation of speech disfluencies ("hmm"s and "uh"s), the system allows people to speak normally, without having to adapt to a machine. *See also* Lamo & Calo, *supra* note 201, at 998; BENKLER, ET AL., *supra* note 42, at 264.

223 Lamo & Calo, *supra* note 201, at 996 (referring to commercial bots and their potential harm).

224 *Id*. ("Commercial bots can also cause harm, primarily by tricking and confusing consumers.").

225 Rosenberg, *supra* note 37.

226 *See* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 136 (2018) (referring to the false trust that social robots build. Waldman focuses on physical bots but the insights apply equally to virtual robots).

227 *Id.* at 137.

or use a service.[228] They do so by lying to consumers, luring them with false promises, or encouraging false assumptions.[229] This false information extends to the source of the message and other contextual elements.

Companies may leave the wrong impression among their consumers that there is high demand for their products.[230] Companies can also lead consumers to false assumptions that a public figure or other "opinion leader"[231] honestly endorsed the product. They can utilize general adversarial networks and create "deep fakes" that seem reliable but are not. For example, they can show a video of a public figure using the product, even though it never happened.[232] Such videos are self-authenticating: "The human mind does not easily dismiss them, and if it does, there is some part of it that remains convinced,"[233] and that "make[s] dissemination of misinformation even easier than before."[234] Alternatively, companies can influence consumers by targeting them with a video in which an opinion leader endorses a product, without disclosing the fact that the company paid him for the endorsement. Thus, for example, some well-known

---

[228] This tool of influence focuses on the information that a consumer receives from a company, as opposed to non-informational elements of the transaction such as engineering emotions and fostering a false sense of trust. On non-informational influences see Berman, *Manipulative Marketing, supra* note 45.

[229] Susser et al., *supra* note 32, at 18.

[230] *See* Arunesh Mathur et al*., Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 81 PROC. ACM HUM. COMPUT. INTERACT. 21 (Nov. 2019).

[231] *See* Everett M. Rogers & David G. Cartano, *Methods of Measuring Opinion Leadership*, 26 PUB. OP. Q. 435, 435 (1962) (highlighting the importance of the source of this message, as "opinion leaders" are individuals who "exert an unequal amount of influence on the decisions of others.").

[232] Robert Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1760 (2019) (raising the problem of deep fakes that are created by general adversarial neural networks and seem to be reliable despite not reflecting the truth). Neural networks can also be used for AI creation of news stories that mimics the style and substance of real news stories. *See* Rowan Zellers et al., *Grover: A State-of-the-Art Defense Against Neural Fake News,* GROVER, https://rowanzellers.com/grover/ [https://perma.cc/6HV7-Z2QC].

[233] *See* CASS R. SUNSTEIN: LIARS FALSEHOODS AND FREE SPEECH IN AN AGE OF DECEPTION 119 (2021); ARAL, *supra* note 130, at 54 ("[T]hat's the future of reality distortion in a world with exponentially improving GANs technology.").

[234] *See* Jon M. Garon, *When AI Goes to War: Corporate Accountability for Virtual Mass Disinformation, Algorithmic Atrocities, and Synthetic Propaganda*, 49 N. KY. L. REV. 181, 183 (2022).

influencers and celebrities have done sponsored posts to promote Honor, a Chinese smartphone manufacturer.[235] Companies can also order their employees to seed messages on message boards and other forums without disclosing that they post on behalf of the platform or an advertiser.[236] These strategies may induce trust in subliminal ways and increase consumers' connection to the brand.[237] Yet, the trust is based on misleading information.[238]

Companies can also enhance the quantity of a commercial message by using AI agents. The previous subsection focused on the qualitative human*ish* characteristics of these agents.[239] Yet, these agents also increase quantity, credibility and visibility of messages. They promote fake news and retweet one another.[240] Bots generate overwhelming amounts of messages to silence counter voices and confuse the public.[241] For example, a user may select a product because it appears at the top of search engine results; however, that placement may be a result of bot manipulation. Similarly, a user may see a tweet because it was re-tweeted many times, unaware that it was retweeted first by an army of bots.[242] As ideas circulate and people repeat them, they tend to gain credibility, even if they are

---

235 *See* 12 Influencer Marketing Examples to Get Inspired By, DIGITAL MARKETERS WORLD (May 13, 2022), https://digitalmarketersworld.com/influencer-marketing-examples/ [https://perma.cc/XL2Z-8LKE].

236 *See* SARAH T. ROBERTS, BEHIND THE SCREEN: CONTENT MODERATION IN THE SHADOW OF SOCIAL MEDIA 141 (2019) ("Online Experts' content moderation employees . . . also actually created new content, seeding sites with messages and discussion points designed to encourage customers' participation and engagement, and to bring a positive face of the brand or product. All of this activity was done surreptitiously without Online-Experts' employees ever identifying themselves as such.").

237 Becher & Feldman, *supra* note 197, at 482.

238 *See generally* Laura E. Bladow, *Worth the Click: Why Greater FTC Enforcement Is Needed to Curtail Deceptive Practices in Influencer Marketing*, 59 WM. & MARY L. REV. 1123 (2018).

239 *See supra* Part I.C(3)b.

240 *See* FRANK PASQUALE: NEW LAW OF ROBOTICS: DEFENDING HUMAN EXPERTISE IN THE AGE OF AI 90 (2020).

241 Tsesis, *supra* note 13, at 1622.

242 LANIER: TEN ARGUMENTS, *supra* note 30, at 55–57; Lamo & Calo, *supra* note 201, at 990 ("[B]ots can create an appearance of false consensus, make a candidate or idea seem more popular than the reality, and even hijack attempts at genuine dialogue and community building."); ARAL, supra note 130, at 48 ("The early tweeting activity by bots triggers a disproportionate amount of human engagement, creating cascades of fake news, triggered by bots but propagated by humans through the Hype Machine's network.")

false or based on false assumptions.[243] Algorithmic dissemination of ideas also misleads viewers into thinking that the ideas are more popular than they actually are.[244]

d) Combining Social Psychology with Cognitive Psychology for Changing Network Dynamics

Companies combine insights of social psychology and cognitive psychology to enhance their influence on the subconscious minds of consumers. They utilize the algorithm to control the context and influence the decision-making processes of individuals by framing what their friends shared. This framing can lead to a cascade of information[245] and enhance structural vulnerabilities that are derived from the fact that individuals are part of a social network.[246]

In an experiment, Facebook researchers manipulated the social and informational content of voting related messages in the news feeds of nearly 61 million Facebook users.[247] Facebook showed one group a statement at the top of their newsfeed encouraging the user to vote. It included a link to polling stations, an actionable button reading, "I voted," a counter indicating how many other Facebook users reported voting, and up to six profile pictures of the user's Facebook friends who had clicked "I voted." A second group received the same information without the pictures of friends. A third group did not receive any messages at all.[248] The group that received the social messages with the profile pictures was about 2 percent more

---

[243] *See* SUNSTEIN, *supra* note 233 at 86 ("The problem is that social cascades, both informational and reputational, can lead to widespread factual errors. Numerous people can end up seeming to believe, or actually believing, something that is not true."); Gordon Pennycook et al., *Prior Exposure Increases Perceived Accuracy of Fake News,* J. EXPERIMENTAL PSYCH. 1865, 1865 (2018).

[244] *See* Kerri A. Thompson**,** *Commercial Clicks: Advertising Algorithms as Commercial Speech*, 21 VAND. J. ENT. & TECH. L. 1019, 1028 (2019).

[245] *See* Cass R. Sunstein & Reid Hastie, *Four Failures of Deliberating Groups* 2 (Univ. of Chi. Pub. Law, Working Paper No. 215, 2008) (explaining that informational cascades are generated when individuals follow the statements or actions of predecessors and do not express their opposing opinions because they believe their predecessors are right).

[246] Nissenbaum et al., *supra* note 32, at 40 (explaining structural vulnerabilities).c

[247] *See* Zoe Corbyn, *Facebook Experiment Boosts US Voter Turnout,* NATURE (Sept. 12, 2012) [https://perma.cc/M5LL-HTSN].

[248] ZUBOFF *supra* note 4, at 299; Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. 335, 335 (2014).

likely to click the "I vote" button than the third group that did not receive any message, and 0.26 percent more likely to click on polling information than the second group that received only informational message. Researchers cross-referenced names with actual voting records and found that those people who saw posts that their friends voted were more likely to vote.[249] The experiment succeeded due to social cues that "primed" users in ways that turned their real-world behavior into a specific set of actions determined by the experimenters.[250]

Similarly, companies utilize algorithms to prioritize newsfeed content created by a user's close friends and family.[251] A user who sees a close friend endorsing a product or clicking "Like" on a company's page is more likely to share the positive information on a product with his friends. The algorithmic framing of endorsement improves older practices of word-of-mouth marketing.[252] It can start an e-word-of-mouth informational cascade, in which other friends follow the endorsement because they believe that if their friend shares the information, it is of value.[253] Consequently, the friends will share the positive information and may even decide to make a purchase accordingly. Companies utilize this strategy to frame an endorsement of an influential member of the social network, since his endorsement is often equivalent to a peer recommendation, and it carries significant weight among his followers.[254]

---

[249] Zittrain, *supra* note 248, at 336.

[250] ZUBOFF, *supra* note 4, at 300.

[251] *See* CASS SUNSTEIN, REPUBLIC: DIVIDED DEMOCRACY IN THE AGE OF SOCIAL MEDIA 16 (2017).

[252] *See, e.g.*, Robert Sprague & Mary Ellen Wells, *Regulating Online Buzz Marketing: Untangling a Web of Deceit*, 47 AM. BUS. L. J. 1, 2–3 (2010) (expanding on word-of-mouth marketing, known as buzz-marketing, which is based on the influence of social networks).

[253] *See* Ravi Sharma, Miguel Morales-Arroyo, & Tushar Pandey, *The Emergence of Electronic Word-Of-Mouth as a Marketing Channel for the Digital Marketplace*, 6 J. INFO. TECH. & ORGS. 41, 41 (2012); Christy M.K. Cheung & Matthew K.O. Lee, *What Drives Consumers to Spread Electronic Word of Mouth in Online Consumer-Opinion Platforms*, 53 DECISION SUPPORT SYS. 218, 219 (2012).

[254] *See* Marty Swant, *Twitter Says Users Now Trust Influencers Nearly as Much as Their Friends*, ADWEEK (May 10, 2016); Bladow, *supra* note 238, at 1128.

II. Manipulation – MORE Than Influence

A. The Elements of Manipulation

Companies not only persuade consumers, but also exploit their vulnerabilities and even create new ones.[255] They target the intuitive, emotional, and instinctive mode of thought, and manipulate them.[256]

What is manipulation? Many legal scholars recognized similar elements when they were pushed to define the concept. Sunstein defines manipulation as an influence on people's choice "to the extent it does *not sufficiently engage with their capacity for reflection and deliberation.*"[257] Susser, Roessler, and Nissenbaum define manipulation as an intentional attempt to influence the subject that (1) is hidden, (2) attempts to exploit a subject's "cognitive, emotional, or other decision-making vulnerabilities," and (3) is "targeted" at those vulnerabilities.[258] Similarly, Calo refers to influencing subjects by (1) targeting the subjects' tendencies to act irrationally and (2) exploiting those tendencies for the manipulators' own gain.[259] Posner refers to the dictionary: "to control or play upon by artful, unfair, or insidious means especially to one's own advantage."[260] It brings "incorrect assumptions to a transaction and does not correct them, or else anticipates and takes advantage of people's propensity to make

---

255 KAHNEMAN, *supra* note 134.

256 CASS SUNSTEIN, THE ETHICS OF INFLUENCE – GOVERNMENT IN THE AGE OF BEHAVIORAL SCIENCE 80 (2016) [hereinafter SUNSTEIN: THE ETHICS OF INFLUENCE]; Cass R. Sunstein, *Fifty Shades of Manipulation,* 1 J. MKTG. BEHAV. 213, 222 (2015) ("Manipulators often target System 1, and they attempt to bypass or undermine System 2.").

257 SUNSTEIN: THE ETHICS OF INFLUENCE*, supra* note 256, at 82; Zarsky*, supra* note 24, at 160 (adopting the same definition as Sunstein, defining manipulative actions as "intentional measures that do not sufficiently engage or appeal to the individual's capacity for reflection and deliberation.").

258 Susser et al., *supra* note 32, at 23; Spencer*, supra* note 33, at 985–86; *see* Kilovaty, *supra* note 132, at 464 (adopting this definition from Nissenbaum).

259 Calo, *Digital Market Manipulation, supra* note 31, at 1001; Spencer*, supra* note 33, at 980 ("Marketers can already identify some individual biases and vulnerabilities in real time, and the emerging research suggests that they will rapidly expand their ability to do so.").

260 Eric A. Posner, *The Law, Economics and Psychology of Manipulation* (University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 726, 2015).

incorrect inferences."[261] Becher & Feldman refer to seven elements of manipulation that relate to the seller's knowledge and motivation.[262]

Spencer reviews common definitions of manipulation and notes that all of them share several features: circumvention of the subject's rational decision-making process or exploiting his vulnerabilities and intention to manipulate.[263] Thus, he defines manipulation as an *intentional* attempt to influence a subject's behavior by *exploiting a bias or vulnerability*.[264]

1. Manipulation and Other Forms of Influence

Manipulation is different from other forms of influence. In contrast to persuasion and coercion, it has a hidden nature that is not in plain sight.[265] Persuasion changes someone's mind by giving reasons, or incentives that he can reflect and evaluate. It leaves the choice entirely up to him. Coercion on the other hand eliminates other "acceptable alternatives" and deprives a person of choice, forcing him to abandon his self-chosen ends.[266] Whereas persuasion and coercion work by appealing to the target's capacity for conscious decision-making, manipulation subverts that capacity. It neither convinces the target (leaving all options open) nor compels him (eliminating all options but one). Instead, it interferes with the target's decision-making process in order to steer him toward the

---

261 *Id.*

262 Becher & Feldman, *supra* note 197, at 475–476 (explaining that the seller must be aware of the vulnerability, be able to exploit the vulnerability, have a profit motive, and be prepared to ignore the consumer's self-interest if necessary. Other related factors of manipulation relate to the exploitive tactics and the unawareness of the consumer); s*ee* Spencer*, supra* note 33 at 984–88 (reviewing elements of manipulation and definitions in scholarship).

263 Spencer*, supra* note 33, at 985; *see also* Jack M. Balkin, *To Reform Social Media, Reform Informational Capitalism*, *in* SOCIAL MEDIA, FREEDOM OF SPEECH AND THE FUTURE OF OUR DEMOCRACY 11 (Lee Bollinger & Geoffrey R. Stone, eds., 2022) ("Manipulation means using a person's emotional vulnerabilities or cognitive limitations against them to benefit the manipulator (or the manipulator's contractual partners) and harm the person manipulated.").

264 Spencer*, supra* note 33, at 990.

265 Susser et al. *supra* note 32, at 14 ("[W]hen we persuade someone to do something (or to refrain from doing it) we appeal, openly, to their capacity for conscious deliberation and choice. We offer arguments or incentives.").

266 *Id*.

manipulator's ends.[267] For example, deceiving someone, or lying to him.[268] Inducing a person to act under false pretenses and enlisting falsehoods at the service of the liars' goal[269] are powerful tools of manipulation.

Nudging is another technique in the toolkit of manipulation. The term "nudge" refers to "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives."[270] Companies can exploit cognitive biases by changing the context in which people make decisions.[271] Not all nudges are manipulative; nudges and manipulation overlap in influencing decision-making without force and by leveraging cognitive biases.[272] Unlike manipulation, a nudge can be transparent.[273] When nudges influence in a hidden manner, they are a form of manipulation.[274]

2. Manipulation and Advanced Technologies

Digital manipulation differs from traditional manipulation, because the message can be tailored to a specific individual and changed by feedback from peers.[275] Digital tools enable the identification of consumers' vulnerabilities, which can be used for manipulation. Anything consumers do near a "linked device" can be tracked. It takes little effort to identify vulnerabilities because technology mediates every aspect of consumers' lives, allows limitless opportunities to impose hidden influences, and exploits consumers' vulnerabilities.[276] In contrast to traditional static advertising, today's

---

267 *Id*.; *see also* SUNSTEIN, *supra* note 256, at 88 (citing JOSEPH RAZ, THE MORALITY OF FREEDOM 377–79 (1986)).

268 *Id.* ("[P]eople may deceive in order to manipulate, but that manipulation does not require instilling false beliefs.").

269 *Id*.

270 *See generally* THALER & SUNSTEIN, *supra* note 135 (discussing nudges).

271 Susser et al., *supra* note 32, at 23; *see also* Richards & Hartzog, *supra* note 128, at 13.

272 Susser et al. *supra* note 32, at 23.

273 SUNSTEIN, *supra* note 256, at 17.

274 *Id*. at 82.

275 Zarsky*, supra* note 24, at 169.

276 Susser et al., *supra* note 32, at 34.

ads are dynamic, interactive, intrusive and personalized.[277] The scope of their influence is greater as they hyper-manipulate consumers, direct the attention, and engage with their intentions.

Consumers do not notice the technological tools, or the fact that companies collect and analyze their data.[278] Even if the attempts to influence are transparent, there may still be a hidden element that affects the subconscious.[279] Consumers cannot fully understand the reason for manipulation, or at least are not always aware of why they receive *specific* advertisements in a *specific* time and place.[280] They are unaware of how specific types of manipulation influence their subconscious.[281] The fact that technology mediates people's lives means that the reach of online manipulation is almost limitless.[282] Manipulation is incidental to the use of connected technologies that makes manipulation cheap and easy, and consumers would have a difficult time to positively choose not to choose to be manipulated because it is part of everyday use of technology.[283]

---

[277] *Id.* at 31–32 ("Unlike traditional advertisements, which were static and disseminated *en masse*, digitally-mediated platforms, such as websites and social media applications, constitute dynamic, interactive, intrusive, and personalized choice architecture.").

[278] *Id.* at 27–28.

[279] For example, in the case of graphic warnings, see Sunstein, *Fifty Shades*, *supra* note 256, at 239 (some forms of manipulation are egregious, as where a vivid, graphic description of an outcome (winning the lottery, dying in an airplane crash, losing a child) is invoked in order to convince people to engage in certain conduct (to buy a lottery ticket, to take a train, to buy extra life insurance)).

[280] Susser et al., *supra* note 32, at 28

[281] SUNSTEIN, *supra* note 256, at 102 ("[T]he idea of manipulating is something taken to imply a lack of transparency, as if something important is being hidden or not being disclosed, and often it is crucial that manipulators are hiding something . . . with respect to manipulation, however, it is not entirely clear what transparency even means. Transparency about what exactly? About the manipulation, own actions? About some aspect of the situation? About the reason that an influence turns out to work? About something else?").

[282] *Id*. ("Unlike 'offline manipulation,' which is constrained by the manipulator's ability to understand and influence a finite number of other people, online manipulation is practically unbounded.").

[283] *See* Michal S. Gal & Niva Elkin-Koren, *Algorithmic Consumers*, 30 HARV. J. L. & TECH. 1, 10–17 (2017) (describing the phenomenon of digital assistants, which represent cases of delegation of authority to technology, and thereby, choosing not to choose). This Article will not focus on the choice to use digital assistants. This issue of delegation of authority raises its own problems and should be examined in a separate study. *See generally* Michal S. Gal, *Algorithmic Challenges to Autonomous Choice*, 25 MICH. TECH. L. REV. 59 (2018).

3. What's Wrong with Manipulation in a Connected World?

a) Autonomy and Dignity

Isaiah Berlin famously defined autonomy as imposing a requirement that a person be "an instrument of [his] own, not other men's acts of will, an individual must be the ruler of his legal right in order for the right to exist as his, free of interference by others or by the government."[284] Manipulation strikes at consumers' autonomy and dignity. Manipulation infringes on the ability of a person to make informed decisions regarding one's life.[285] It bypasses reflective thinking and hinders personal autonomy to choose between options.[286] It deprives a person of his capacity to decide for himself, and the opportunity for self-authorship over a person's own actions.[287] Arguably, limiting the capacity to choose infringes on autonomy.[288] Manipulation may also humiliate an individual and trample on his dignity by subverting deliberative thinking.[289]

The relationships between companies and consumers are asymmetric in digital markets,[290] thus manipulation causes greater harm to the consumers' autonomy.[291] Engineers design automated

---

[284] *See* ISAIAH BERLIN, LIBERTY 178 (Henry Hardy 1969).

[285] Zarsky, *supra* note 24, at 174 ("[T]he manipulative steps here discussed lead individuals to exercise first-order preferences that they might find acceptable at the moment, yet are not in step with their second-order preferences."); *see also* GERALD DWORKIN, THE THEORY AND PRACTICE OF AUTONOMY (1988).

[286] *Id.* at 173; Calo, *supra* note 31, at 1031; Gideon Parchomovsky & Alex Stein, *Autonomy*, 71 TORONTO L.J. 61 (2021) (explaining that every infringement of a right involves an infringement of autonomy).

[287] Gal, *Algorithmic Challenges to Autonomous Choice, supra* note 284, at 79.

[288] Susser et al., *supra* note 32, at 2 (giving the example of Facebook that targets ads to vulnerable teens and arguing that the suspicion is that they are doing this to exploit the teen's moment of weakness, not to remedy it, and to influence them to buy something they don't need or to pay more for it than they otherwise would).

[289] KAHNEMAN, *supra* note 134 (referring to the intuitive system and deliberative mode of thought).

[290] ZUBOFF *supra* note 4, at 11 ("[S]urveillance capitalism operates through unprecedented asymmetries in knowledge and the power that accrues to knowledge.").

[291] SUNSTEIN, THE ETHICS OF INFLUENCE, *supra* note 256, at 97 (explaining that this role and position of companies matters in the assessment of manipulation; for example, if a person is trying to obtain a job by causing a prospective employer to like him by appealing to his intuitive thinking, it would be legitimate for him to take advantage of social influence, unless he were to lie and deceive the prospective employer; in different power relations, manipulation might not be considered ethical); ZUBOFF, *supra* note 4, at 233–42,

technology to influence and modify human behavior.[292] Mass behavior modification threatens consumers' autonomy at scale and in depth. The more companies collect and analyze data, the more they can modify behavior. As Zuboff describes, the manipulative practices of companies suffocate autonomy and infringe on consumers' "will to will," because companies shape their commercial opportunities by their previous activities and reactions to advertisements.[293]

b) Welfare and Efficiency

Liberal philosophy assumes that individuals know what is subjectively best for them.[294] However, it might not always be so. Individuals have their biases; and, at times, they lack the relevant information to reach decisions.[295] Manipulating their choices does not always reduce welfare and can even increase it by tailoring services to each consumer's preferences.[296] Therefore, from a welfare standpoint, manipulation is not necessarily objectionable.[297] The main problem is that manipulators have their own agendas,[298] which are not necessarily meant to benefit the individual.

Successful manipulation can generate a suboptimal transaction, in which companies target consumers against their interests as they fail to exercise their long-term preferences.[299] Consequently,

---

299 (referring to the role of manipulator and the asymmetry of knowledge and power and to experiments that social media intermediaries conduct on their users by utilizing this asymmetry of power); *see also* Eliza Mik, *The Erosion of Autonomy in Online Consumer Transactions*, 8 L. INNOVATION & TECH. 1, 2 (2016).

292 ZUBOFF, *supra* note 4, at 150.

293 *Id.* at 291.

294 Sunstein, *Fifty Shades*, *supra* note 256, at 213 ("To that extent, the central objection to manipulation is rooted in a version of John Stuart Mill's Harm Principle: People know what is in their best interests and should have a (manipulation-free) opportunity to make that decision.").

295 Gal, *Algorithmic Challenges, supra* note 284, at 77.

296 Sunstein, *Fifty Shades*, *supra* note 256, at 228 ("Manipulation might promote people's welfare.").

297 *Id.* (explaining that it can be argued that the utility argument is uncertain and some consumers might benefit from manipulation).

298 Calo, *supra* note 31, at 1023 (explaining that companies are coupled with divergent interests that should raise a red flag).

299 Susser et al., *supra* note 32, at 6 (giving example of Facebook that targets ads to vulnerable teens). The suspicion is that they are doing this to exploit the teen's moment of

consumers are manipulated to purchase products they don't need, leading to waste and inefficiency.[300] Take, for example, the New York Times reporter Brian Chen.[301] After deleting his Facebook account, he stopped seeing relevant ads that previously seduced him to buy things he did not need.[302] Consequently, his online shopping purchases dropped by 43 percent.[303]

Manipulated consumers do not necessarily act against their preferences, but rather change them. As Posner explains, even if individuals take self-protective measures that protect them from manipulative steps, such measures are both costly and time-consuming, thus generating waste and decreasing welfare.[304]

Whether manipulation is objectionable from a welfare or economic standpoint depends on the context.[305] However, suspicion surrounding manipulators' goals is justified.[306] Whereas the consumer strives to purchase useful products, the agenda of a manipulator is to maximize his profits. The designers and operators of technologies construct a digital environment that will subordinate consumers' interests to theirs. [307]

There are also broader macro-level costs and risks. Manipulation extends beyond the decision of individuals and can affect markets as a whole. It can hinder competition and impose a massive burden

---

weakness, not to remedy it, and to influence them to buy something they don't need or to pay more for it than they otherwise would.

300 Zarsky, *supra* note 24, at 172; Calo, *supra* note 31, at 1025.

301 *See* Brian X. Chen, *I Deleted Facebook Last Year, Here's What Changed (and What Didn't),* N.Y. TIMES (Mar. 21, 2019), https://www.nytimes.com/2019/03/21/technology/personaltech/facebook-deleted.html [https://perma.cc/86EH-44PR].

302 *Id.*

303 *See id.* ("[I]nstagram might have started thinking I was female, but my wallet thanked me. I realized I was spending considerably less money on my usual guilty pleasure of buying clothing and cooking gadgets online because I was no longer seeing the relevant Facebook ads that egged me on to splurge.").

304 Posner, *supra* note 260, at 9; Zarsky, *Privacy and Manipulation, supra* note 24, at 173.

305 SUNSTEIN, *supra* note 256, at 100–01 (giving an example of graphic health warnings for example against smoking; in such context, manipulation might increase welfare and is not objectionable).

306 *Id.*

307 Susser et al., *supra* note 32, at 35.

on the least sophisticated consumers.[308] It can also be a source of a market failure; because, if some market actors utilize bias and get the results they want, those vendors who do not utilize such biases find themselves ejected from the market.[309]

Manipulation can completely transform the structure of markets and business.[310] Media giants such as Facebook and Google have a business advantage in magnitude and network. They can use the data collected from users to manipulate consumers.[311] By choosing what to advertise, these media giants might get control over what is offered to consumers and thereby undermine the stability of other markets.

c) Democracy and Self Governance

Manipulation in digital markets causes harm to democracy and democratic institutions. This is true in both political and commercial contexts.[312] By hindering reflective thinking without transparency, manipulation threatens democratic principles of autonomy of citizens and their ability to be engaged in democratic deliberation.[313]

This new economic order infringes on democratic values of self-governance, the capacity to form ideas, and participatory culture as

---

[308] Calo, *supra* note 31, at 1026 (referring to OREN BAR GIL, SEDUCTION BY CONTRACT: LAW ECONOMICS AND PSYCHOLOGY IN CONSUMER MARKETS (2012).

[309] *Id.* at 1001.

[310] *See generally* Rory Van Loo, *Digital Market Perfection*, 117 MICH. L REV. 815 (2019) (explaining that AI recommendations can change markets and industrial organization).

[311] Daniel Susser et al., *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1, 29–30 (2019) ("Both the information [we] knowingly disseminate about [ourselves . . . when we] visit websites, make online purchases, and post photographs and videos on social media[,] and the information [we] unwittingly provide . . . as those websites record data about how long [we] spend browsing them, where [we] are when [we] access them, and which advertisements [we] click on[,] reveals a great deal about who [we are], what interests [us], and what [we] find amusing, tempting, and off-putting.")

[312] *See, e.g.*, Turow, *supra* note 16; BENKLER, ET AL., *supra* note 42 (expanding on manipulation in political contexts and the harm to democracy).

[313] Kilovaty, *supra* note 132, at 471; *see also* Susser et al., *supra* note 32, at 37; ZUBOFF *supra* note 4, at 11 (explaining that the force of surveillance capitalism "nullif[ies] elemental rights associated with individual autonomy that are essential to the very possibility of democratic society").

it is reflected in free participation in shopping, by deciding autonomously which products to buy.[314]

4. Should the Law Limit Manipulation? Does the Law Already Pose Limitations on Manipulation?

Manipulation is not inevitable. It is the product of conscious design choices, "carefully studied and tested to maximize their effectiveness in shaping targets' choices without those targets' conscious awareness."[315] How should the law react to manipulation? Should it pose limitations on manipulation? Should the law impose liability on those who manipulate consumers, even if the manipulation does not violate any specific law?

Scholars are concerned about advanced strategies of manipulation, which are based on technology and data driven practices.[316] Professor Jack Balkin offered scholars to apply information fiduciary duties on intermediaries.[317] This concept likens digital company's obligations towards its users' information to the fiduciary duties of doctors or lawyers towards patients and clients. Digital

---

[314] TUROW, *supra* note 19, at 46 (explaining that when others have access to our private information, they are able to influence or control our actions and our capacity to form ideas, experiment, think or to make mistakes without observation or interference by others. Turow also refers to inequality and price discrimination as a threat to democracy in markets).

[315] *See* Helen Norton, *Manipulation and the First Amendment*, 30 WM. & MARY BILL RIGHTS 221, 229 (2021).

[316] *See, e.g.*, Calo, *supra* note 31, at 1025–34 (expanding on the potential harm of manipulation in digital markets); *see also* Susser et al., *supra* note 32, at 2 ("Privacy and surveillance scholars increasingly worry that data collectors can use the information they gather about our behaviors, preferences, interests, incomes, and so on to manipulate us."); Becher & Feldman, *supra* note 197, at 494 ; Berman, *Manipulative Marketing, supra* note 45, at 520.

[317] *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186–87 (2016); Jack M. Balkin, *Fixing Social Media's Grand Bargain*, *in* AEGIS PAPER SERIES 2018 11 (Hoover Inst., Aegis Series Paper No. 1814, 2018); Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11, 16 (2020); Jack M. Balkin, *To Reform Social Media, Reform Informational Capitalism in Social Media, Freedom of Speech and the Future of Our Democracy* 125 (Lee Bollinger and Geoffrey R. Stone, eds.) (forthcoming) ("Fiduciary duties apply not only to social media companies, but to any companies that collect and monetize end-user data. This is important because the internet of things allows many different objects and appliances to collect personal data. Fiduciary duties must also apply to smart homes, self-driving cars, and personal digital assistants.").

companies can be likened to fiduciaries because, much like lawyers and doctors, they receive—and even actively collect—personal information on the individuals that use their services and they are trusted to treat this information with care.[318] Users have little knowledge about the digital company, its operations, the data it collects, how data is used, and how data is shared. Due to this asymmetry, users are particularly vulnerable and naively trust the companies, believing they will not betray their trust or manipulate them. Under this concept, intermediaries should neither breach users' trust, nor take actions that users would reasonably consider unexpected or abusive. In other words, companies should act in good faith and avoid manipulation.[319] Yet, this concept is vague and is difficult to apply.[320] It also requires concretization since manipulation is everywhere and one cannot forbid it altogether. Richards and Hartzog tried to outline nuanced duties of loyalty to act in the best interest of consumers and avoid conflict of interest on two levels: a general prohibition on substantial conflicts with the trusting party's best interests, and specific duties targeting actions.[321] However,

---

[318] Balkin, *The Fiduciary Model of Privacy*, at 11 ("[T]he law should treat digital companies that collect and use end user data according to fiduciary principles.").

[319] *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1229 (2016); *see also* Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy,* ATLANTIC (Oct. 3, 2016), www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/ [https://perma.cc/DD95-8NU3]; Richards, *supra* note 20, at 63 n.3 (referring to laws to impose duties of loyalty).

[320] *See* Lina M. Khan & David E. Pozen*, A Skeptical View of Information Fiduciaries,* 133 HARV. L. REV. 497, 524 (2019) (outlining tensions and ambiguities in the theory of information fiduciaries, as well as a number of reasons to doubt the theory's capacity to resolve them satisfactorily); *see also* Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics,* 79 MD. L. REV. 439, 470 (2020) (explaining that companies that collect information are in many instances not the same companies that manipulate and the concept of consent to disclosure in fiduciary relations does not fit well with the developments of technology).

[321] Woodrow Hartzog & Neil Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 356, 371 (2022).

loyalty obligations are still vague[322] and it is not always clear what is the best interest of the consumer.[323]

Another proposal to tackle manipulation focuses particularly on abusiveness in interfaces and designs that interfere with people's ability to decide who to trust within consumer regulation. Neil Richards proposed that privacy law should ask whether a particular design interferes with our understanding of risks or exploits our vulnerabilities in unreasonable ways.[324] However, this proposal leaves vagueness regarding which exploitations of vulnerabilities should be regulated.

Other scholars offer to push the boundaries of law and adopt a holistic approach for regulating manipulation. Becher & Feldman propose a continuum of regulatory reactions to non-verbal manipulation that would allow flexibility.[325] Such regulatory reactions include *ex ante* regulation to ban manipulation unless an administrative agency pre-approved it, a safe haven for pre-approving commercial practices, or *ex post* facto legal suits of consumers.[326] Other regulatory actions include disclosure requirements[327] and the right to cancel a transaction,[328] especially when the manipulative architecture doubles the likelihood of buying relative to neutral interfaces.[329]

---

322 *See* Richards & Hartzog, *supra* note 128, at 1013 ("When companies are not told exactly what they need to do to comply, they are likely to err on the side of caution and exercise more restraint than just getting 'right up to the creepy line and not cross[ing] it.'"); Hartzog & Richards, *Legislating Data Loyalty*, *supra* note 321, at 356.

323 Richards & Hartzog, *supra* note 128, at 992 ("[A] best-interests approach has its own undeniable vices.").

324 RICHARDS, *supra* note 20, at 195–96.

325 Becher & Feldman, *supra* note 197, at 488, 491 (focusing on non-verbal manipulation and reflecting in their proposal on the existence of different degrees of manipulation, the level of harm, the level of unfairness and the public targeted.).

326 *See id*. at 488–89 (explaining that this approach places the burden to file an action on consumers and can encounter difficulties. Consumers are usually unaware of the manipulation, or cannot connect it with an infringement of their rights. Furthermore, they are likely to avoid costly litigation, or fail to prove manipulation).

327 *See id*. (referring to the limitations of this solution due to the ubiquitous nature of non-verbal manipulation and the limitations of disclosure obligations in general.).

328 *See id.* at 490 (explaining that this solution might not work due to the endowment effect and transaction costs.).

329 Luguri & Strahilevitz, *supra* note 85, at 81 (explaining that manipulation in the architecture of a website that doubles the likelihood of a purchase should constitute grounds

Should the law regulate new forms of manipulation? Policy makers should ask whether new forms of manipulation require regulatory intervention.[330] What are the challenges in restricting manipulation?

d) Challenges to Legal Restrictions on Manipulation

i. Autonomy Cannot Be Limitless

Every manipulation infringes on autonomy; yet, a person's autonomy is not absolute. Interactions of individuals with others involve mutual commitments such as contracts and engagements that change the scope of autonomy.[331] In fact, every right an individual possesses infringes on the autonomy of another.[332] Protection of autonomy should be a matter of degree, as there are different degrees of autonomy and it cannot be protected fully.[333] Eliminating old and new forms of manipulation altogether is undesirable. To do so would hinder free speech, the free flow of information, and the freedom of companies to do business.[334]

ii. Fifty Shades of Manipulation, Fifty Degrees of Influence

Imposing legal limitations on manipulation is a challenge. Policymakers must decide what to regulate.[335] As discussed previously, there are many forms and degrees of manipulation:[336] it is everywhere, with many nuances and countless social contexts.[337] Not all

---

to nullify the contract because it is more likely than not that the manipulation caused the consumer to buy a product he did not want).

330 Zarsky, *supra* note 24, at 171.

331 Parchomovsky & Stein, *supra* note 286, at 9.

332 Gal & Elkin-Koren, *Algorithmic Challenges, supra* note 283, at 103 (explaining that state-imposed limitations such as intellectual property rights harm the autonomous right to exercise free speech; thus, individual autonomy cannot be limitless).

333 *See* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE AND THE PLAY OF EVERYDAY PRACTICE 16–21 (2012).

334 Zarsky, *supra* note 24, at 174 (establishing the acceptable extent of harm to autonomy in every context is complicated).

335 Spencer, *supra* note 33, at 993 (addressing the challenges of regulation of online manipulation).

336 *See* Part I.C.

337 *See* Sunstein, *Fifty Shades*, *supra* note 256, at 80–83 (explaining that there are many nuances of manipulation).

forms of digital manipulation were created equal: some manipulative influences are deep while some are shallow.

Studies demonstrate that psychographic data is more effective than other marketing techniques.[338] However, studies also suggest that concerns regarding psychographic profiles are unfounded because experiments that matched personality types to advertisements did not significantly alter click-through rates.[339] There was a 1.54 increase in actual purchases among those who did click through, yet out of *three million* people that researchers tried to manipulate, only 390 individuals actually purchased the product.[340] Moreover, manipulation can influence the decision making of one person while having no effect on another, because not everyone has the same biases.[341] Differentiating between types and shades of manipulation is a difficult task, especially given the evolving state of psychological and neuro-marketing research.[342]

iii. The Causal Link Between Manipulation and Decision-Making

Manipulation influences part of the target audience. The fact that a person was exposed to manipulation and then bought a product does not necessarily mean it was the manipulation that caused the purchase. Other factors may have influenced his decision. In a related context of targeting and manipulating voters to achieve political goals for example, Cambridge Analytica that targeted voters in the 2016 U.S. election by using psychological data, harvested largely without permission, was not the only factor that influenced voters.

338 *See* Wu Youyou, Michal Kosinski, & David Stillwell, *Computer-Based Personality Judgments Are More Accurate Than Those Made by Humans*, 112 PROC. NAT'L ACAD. SCI. 1036, 1036–40 (2015).

339 BENKLER, ET AL., *supra* note 42, at 277.

340 *Id.*

341 Spencer*, supra* note 33, at 977.

342 Berman, *Manipulative Marketing, supra* note 44, at 536.

Rather, there were external influences independent of the manipulation,[343] such as social pressures and reputation cascades.[344]

Similarly, in the context of manipulation of commerce, the consumer might have bought the item anyway without the manipulation, as he brings his own set of preferences to the transaction.[345] How can private actors file an action without being able to demonstrate a causal link between the manipulation and its effects? In addition, it is difficult to prove a causal connection between the prohibited conduct and harm to consumers. This might doom any private right of action in federal court due to lack of standing.[346] Technology makes it possible to conduct wide-scale online experiments regarding patterns and to reveal the most influential dark patterns.[347] Yet these experiments fall short when it comes to personalized targeting of vulnerability, making it difficult to prove the question of causal connection.

iv. Getting Remedies Without Having a Right to be Free from all Forms of Manipulation

Assuming that a person who has been manipulated would not have bought the product without manipulation, there remains the question of recognizing a violation of a right. Manipulation surrounds our everyday lives. Some forms of manipulation are a part of any discourse,[348] so it is impossible to prohibit manipulation

---

343 *See* BENKLER, ET AL., *supra* note 42, at 225–26 (explaining that the narrative that followed the 2016 elections emphasized Facebook's advertising and Russian propaganda; ideological news websites also play a role in information dissemination on the social network and the structure of the social network is also an influential factor; Benkler even argued that in the context of the 2016 campaign election the structure of the social network is the most important factor.).

344 *See* Sunstein & Hastie, *supra* note 245 (manipulation can trigger information and reputation cascades, yet cascades can form regardless of manipulation).

345 Spencer*, supra* note 33, at 997.

346 *Id.* at 998*; see* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) ("[Plaintiff] could not, for example, allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III."); *see also* Trans Union LLC v. Ramirez, 141 S. Ct. 2190, 2219–2220 (2021); Daniel J. Solove & Danielle Keats Citron*, Standing and Privacy Harms: A Critique of* Transunion v. Ramirez*,* B.U.L REV. 62, 62 (2021).

347 Luguri & Strahilevitz, *supra* note 85.

348 *See* Zarsky*, supra* note 24, at 184.

altogether.[349] Enforcing an overall right to be free from manipulation would mean chilling speech, hindering personal development,[350] stifling innovation, and curtailing the right of retailers to conduct business.[351]

Recognizing harm to autonomy and efficiency in every case of manipulation would overwhelm courts with suits, leading to exorbitant administrative costs.[352] It could also be argued that the harm of manipulation is de minimis or that it is impossible to quantify the sum of monetary compensation for such harm.

e) Manipulation and the Law

The law generally sticks to the notion that individuals are autonomous,[353] and therefore an individual's capacity for sound judgment is temporarily impaired only in narrow circumstances.[354] Courts usually apply doctrines to restore autonomy or void decisions that infringe upon autonomy.[355] For example, in *Ohralik* v. *Ohio State Bar Ass'n,* the Court upheld sanctions against a lawyer who violated state bar rules by engaging in in-person solicitation, immediately following a car accident ("ambulance chasing").[356] The Court wrote that in-person solicitations were likely to produce "speedy and perhaps uninformed decision making," hindering the individual and societal interest in facilitating informed decision-making.[357]

One interpretation of this diversion from the general autonomy assumption is that the law restricts only unduly coercive methods of

---

349 *See id*.

350 *See* Jonathon W. Penney, *Understanding Chilling Effects*, 106 MINN. L. REV. 1451, 1463 (2022) (explaining that chilling effect leads to social conformity and hinders personal development).

351 Zarsky, *supra* note 24, at 184 ("The prohibition on manipulation, if construed too broadly, might also prove to be a limitation on innovation.").

352 *See* Parchomovsky & Stein, *supra* note 287, at 35.

353 Zarsky, *supra* note 24, at 178.

354 *See id*. at 177 (voiding contracts when the plaintiff proved that the defendant used coercion and undue influence).

355 *See id.* (giving an example of one narrow exceptions–laws regulating advertising); *see also* JOHN A. SPANOGLE ET AL., CONSUMER LAW 68 (3d ed. 2007) (discussing the Federal Trade Commission's authority to act on "unfair" advertisements, despite the fact that it rarely does so, focusing more on deceptive ads).

356 *See* Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 449 (1978).

357 Berman, *supra* note 45, at 505.

communication that exceed the scope of manipulation.[358] Another interpretation of this diversion in *Ohralik* is that, in this case, the individual obtained information from only one source, and he was unable to engage in comparative research, regarding his options.[359]

B. Are There No Other Sources of Information? Is There No Way Out?

Arguably, digital manipulation limits the information available to one source because the network effects of media giants, large retailers, and advertisers limit the available options.[360] A counter argument is that with different business models and agendas, even digital manipulation cannot restrict information to just one source because the digital ecosystem contains various intermediaries. Therefore, the situation is not monopoly-like at this stage. In a connected environment it is easier for a consumer to seek out other options or decide not to buy.[361] Consumers can obtain information from other marginal consumers who have examined the company's conduct *ex ante*[362] or from other consumers that post reviews *ex post*, after completing transactions. As such, consumer organizations also make it easier to pass on information. At the very moment of manipulation, connected devices allow users to make an inquiry on a company, or on a specific deal it offers, as well as other available options.[363] Arguing that other options are unavailable seems far-fetched at this stage.

Another argument against legal sanctions for manipulation is that individuals can adapt to manipulative processes.[364] They can develop resistance to manipulation based on experience or engage

---

358 *See id*.

359 Zarsky, *supra* note 24, at 182 (identifying that in such situations market dynamics fail to occur).

360 *See id.* (giving an example of social networks, search engines, and big retailers).

361 *See* BENKLER ET AL., *supra* note 42, at 277 (describing an experiment in psychographic profiles that led to only marginal increases in actual buying).

362 *See* Shmuel I. Becher & Tal Z. Zarsky, *E-Contract Doctrine 2.0: Standard Form Contracting in the Age of Online User Participation*, 14 MICH. TELECOMM. & TECH. L. REV. 303, 330 (2008).

363 *See generally* Michal S. Gal & Niva Elkin-Koren, *Algorithmic Consumers*, 30 HARV. J.L. & TECH. 309 (2017).

364 Zarsky, *supra* note 24, at 183–84.

in self-correction.[365] Educational methods might also prove effective in creating such resistance.[366] Treating manipulation as a no way-out situation goes too far, and therefore policymakers should exercise caution when restricting it.

1. Existing Legal Limitations on Manipulation

Manipulation is a type of misbehavior. It does not reach the level of coercion or fraud, yet it achieves the same goals.[367] Sunstein has argued that the legal system "usually does not attempt to prevent [manipulation]."[368] Eric Posner disagrees, arguing that specific laws exist to combat particular forms of manipulation, even if the legislature does not formally recognize them as such.[369] Manipulation goes under various other titles such as unconscionability, misunderstanding,[370] bad faith, and deceit. For example, consumer protection statutes prohibit misleading and false statements.[371] Contractual doctrines[372] and rules require disclosure of information.[373]

---

365 *Id.* at 184.

366 *See id.*

367 *See* Posner, *supra* note 260, at 6.

368 *See* SUNSTEIN, *supra* note 256, at 9.

369 *See* Posner, *supra* note 260, at 5.

370 *See id.* (referring to Restatement (Second) of Contracts § 20, which says that if two contractual parties attach different meanings to a term of a contract, the meaning of one party is enforced if the other party knew or had reason to know that the first party attached the different meaning).

371 *See* Ellen P. Goodman, *Stealth Marketing and Editorial Integrity*, 85 TEX. L. REV. 83, 108 (2006); Federal Trade Commission Act, 15 U.S.C. § 45(a)(2) (2000) (giving the Federal Trade Commission the authority to sanction false advertising); Lanham Act, 15 U.S.C. § 1125(a) (2000) (providing a civil right of action for persons injured by "false designation of origin, false or misleading description of fact, or false or misleading representation of fact" with respect to "goods, services, or commercial activities" in "commercial advertising or promotion").

372 *See* Luguri & Strahilevitz, *supra* note 85, at 94 ("[U]ndue influence renders a contract voidable by the influenced party."); Restatement (Second) of Contracts § 177 (1981) ("[U]ndue influence is unfair persuasion of a party who is under the domination of the person exercising the persuasion or who by virtue of the relation between them is justified in assuming that that person will not act in a manner inconsistent with his welfare[.]").

373 *See* Richard Craswell, *Taking Information Seriously: Misrepresentation and Nondisclosure in Contract Law and Elsewhere*, 92 VA. L. REV. 565, 566, 595 (2006); Tal Z. Zarsky, *Serious Notice: A Celebration, Discussion, and Recognition of Joel Reidenberg's Work on Privacy Notices and Disclosures,* 90 FORDHAM L. REV. 1457, 1477 (2022). Litigation is brought by the FTC under Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices." *See, e.g.*, 15 U.S.C. § 45(a)(1)

Additionally, Section 5 of the Federal Trade Commission Act regulates unfair methods of competition affecting commerce, and unfair or deceptive acts or practices affecting commerce, and declares them unlawful.[374] In fact, the FTC's baseline rule is *don't lie*.[375] Restrictions on misrepresentations, false statements, and regulation of disclosures in commercial contexts restrict the exploitation of incorrect assumptions that a consumer brings to the transaction.[376] Under Section 5 of the FTC Act, the FTC is the existing institution best suited to regulate manipulation.[377] States and the federal government have granted consumers special rights in settings characterized by high pressure, mild coercion, or vulnerability, such as door-to-door-sales and transactions involving funeral services, timeshares, telemarketing, or home equity loans.[378] Sometimes the law enacts outright prohibitions with substantial penalties.[379] Where manipulation in markets is a problem, the law regulates it.[380]

Posner has a point. The law restricts some forms of manipulation, even when they do not reach the threshold of fraud, defamation,

---

(2000). In addition, there is litigation brought by private parties under the Lanham Act, which prohibits the sale of products under any false description or representation. 15 U.S.C. § 1125(a)(1) (2000); *see also* Jean Wegman Burns, *Confused Jurisprudence: False Advertising Under the Lanham Act*, 79 B.U.L. REV. 807, 823 (1999).

374 *See* 15 U.S.C. 45(a); CHRIS J. HOOFNAGLE: FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 31–53 (2016).

375 *See id.* at 245; Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 25 (2019); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 629–38 (2014) (reviewing the FTC's deception jurisprudence focusing on incidents of lying and misleading statements in privacy policies).

376 *See* Posner, *supra* note 260, at 6.

377 *See* Luguri & Strahilevitz, *supra* note 85, at 103 (explaining that legal commentators have largely failed to notice that the FTC is beginning to combat dark patterns with some success, at least in court, although it does not use the term dark patterns); FTC v. AMG Cap. Mgmt. 910 F.3d 417 (9th Cir. 2018); FTC v. Off. Depot, Stipulated Order for Permanent Injunction and Monetary Judgment, Case No. 9-19-cv-80431-RLR (S.D. Fla. Mar. 28, 2019) (perceiving dark patterns as lies and misrepresentation).

378 *See* Becher & Feldman, *supra* note 197, at 468.

379 *See* Luguri & Strahilevitz, *supra* note 85, at 46; *see, e.g.*, *FTC Sues Owner of Online Dating Service Match.com for Using Fake Love Interest Ads to Trick Consumers into Paying for a Match.com Subscription*, FED. TRADE COMM'N (Sept. 25, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/09/ftc-sues-owner-online-dating-service-matchcom-using-fake-love-interest-ads-trick-consumers-paying. [https://perma.cc/5KP3-Q8YK].

380 *See* Posner, *supra* note 260, at 1.

or other behaviors that the law explicitly forbids.[381] Yet, at the moment, "manipulation of social media and the virtual world have little, if any, legal consequences". [382] Existing regulation is insufficient to mitigate the harm caused by digital manipulation and does not provide a remedy for individuals who have been manipulated.

However, there have been recent specific proposals that aim to limit manipulation, by focusing on manipulation by algorithms. As the next subsection explains, such proposals are over-broad and might chill desirable uses of technology and market behavior.

2. Overbroad Regulatory Proposals

a) A. Prohibiting Algorithmic Uses That Exploit Vulnerabilities

The E.U. recently proposed regulations that focus on uses of technology. The proposal focuses on Artificial Intelligence ("AI"), classifies AI practices to distinguished categories,[383] and bans certain uses of AI algorithms altogether.[384] In order to ban them, or otherwise impose liability, they should recognize that these AI-centered algorithms *pose unacceptable risks in manipulating human*

---

381 *See* Posner, *supra* note 260, at 4–6

382 *See* Jon M. Garon, *When AI Goes to War: Corporate Accountability for Virtual Mass Disinformation, Algorithmic Atrocities, and Synthetic Propaganda*, 49 N. KY. L. REV. 181, 219 (2022).

383 *See generally* Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM (2021) 206 final (Apr. 21, 2021) [hereinafter Artificial Intelligence Act] (addressing (1) unacceptable risks (Title II); (2) high risks (Title III); (3) limited risks (Title IV); (4) minimal risks (Title IX)). For further information, see Margot E. Kaminski, *Regulating the Risks of AI*, 103 B.U.L. REV. (forthcoming 2023) (at 49–54), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4195066 [https://perma.cc/C9ND-XJNX], and Denise Almeida et al., *The Ethics of Facial Recognition Technologies, Surveillance, and Accountability in an Age of Artificial Intelligence: A Comparative Analysis of US, EU, and UK Regulatory Frameworks*, 2 AI & ETHICS 377 (2022).

384 *See id*.; *cf.* Thomas Burri & Fredrik von Bothmer, *The New EU Legislation on Artificial Intelligence: A Primer*, at 2 (Apr. 21, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3831424 [https://perma.cc/S8XT-JJ26] ("The proposed regulation prohibits certain uses of AI. It bans the use of AI: a) to materially distort a person's behavior; b) to exploit the vulnerabilities of a specific group of persons; c) public social scoring and d) for real time remote biometric identification in public places.").

behavior.[385] So far, the proposed regulation aims to limit manipulation by banning AI uses that materially distort a person's behavior or exploit the vulnerabilities of a specific group of persons.

The E.U. proposal is vague. It is unclear what materially distorts a person's behavior with probable physical or psychological harm[386] or reaches the level of exploiting vulnerability. This type of categorial ban on such AI uses has the capability to risk impairing beneficial uses of AI, which could lead to disproportionate chill on technology, innovation, and even speech.

b) Prohibiting Manipulative Practices

In the United States, legislative proposals seek to regulate manipulative online practices.[387] For example, the Deceptive Experiences To Online Users Reduction Act[388] proposes to prohibit interfaces designed "with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or [the] choice to obtain consent or user data;" practices that "subdivide or segment consumers of online services into groups for the purposes of behavioral or psychological experiments or studies, except with the informed consent of each user involved;" and practices that cultivate children's compulsive platform usage"[389] To allow FTC enforcement, the bill proposes to treat such practices as unfair or deceptive acts or practices in or affecting commerce.[390]

---

[385] Article 5(1) of the Artificial Intelligence Act deals with prohibited AI practices such as an "AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behavior in a manner that causes or is likely to cause that person or another person physical or psychological harm." *See* Artificial Intelligence Act, *supra* note 384, at 43; *see also* Michael Veale & Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, 22 COMPUT. L. REV. INT'L 97, 98 (2021), https://arxiv.org/ftp/arxiv/papers/2107/2107.03721.pdf [https://perma.cc/BJ7K-6XTQ].

[386] *See* Luciano Floridi, *The European Legislation on AI: A Brief Analysis of Its Philosophical Approach,* PHIL. & TECH. 215, 219 (2021) ("[T]he proposal is vague, such as when it comes to banning the use of AI systems intended to distort human behavior, with probable physical or psychological harm. The intent is commendable, but it might risk banning even unproblematic AI systems if this approach were applied in a Draconian way.").

[387] *See* Norton, *supra* note 316, at 234.

[388] *See id*.; S. 1084, 116th Cong. § 3(a)(1) (2019).

[389] *See* Norton, *supra* note 316, at 234.

[390] *See id.;* 15 U.S.C. 45(a)(2) (2000).

Much like the E.U. legislative proposal regarding AI, this bill is also vague and needs concretization, as it is unclear and can hinder a broad set of business models and marketing practices. Efforts to limit manipulation should be clear and nuanced.

III. Regulating Lies and Specific Non- Disclosures (Misrepresentations): From Stealth Marketing Regulation to Mitigation of Manipulation

The law cannot impose liability for every attempt to manipulate and for every infringement of autonomy;[391] rather it should draw the line at regulation of manipulation. This Part proposes specific corporate obligations to avoid lies. In addition, it mandates specific disclosures that aim to mitigate misrepresentation. The proposed obligations expand upon and refine existing restrictions and implicit prohibitions against manipulation and accommodate them to manipulation in data driven markets. Non-compliance with these obligations would lead to public fines and provide individuals with compensation for infringement of autonomy.

A. Ex-Ante Restrictions on Manipulation: A Focus on Lies by Powerful Speakers and Non-Disclosure

Data driven companies enjoy an informational advantage, uneven power relations vis a vis their listeners, and have an augmented capacity to manipulate.[392] Professor Helen Norton explains that in this setting policymakers should adopt a "listener-centered" approach to government regulation.[393] This approach would permit regulation of speech by knowledgeable or powerful speakers when

---

391 *See* Sunstein, *supra* note 256 (explaining that there are many nuances of manipulation). For example, addictive platform features are just one type of manipulation, and proposals to regulate some of the addictive features will not eradicate the problem completely. *See generally* Mettler, *supra* note 55 (a legislative bill proposing to limit addictive platform features).

392 Norton, *supra* note 46, at 443.

393 *See id.* This approach focuses on First Amendment concerns and regulation and this Article will return to these concerns in Part V. This approach also provides independent justifications and boundaries for applying regulation in specific situations and not in others.

their speech frustrates the autonomy and self-governance of their listeners.[394]

Norton suggests a few ways to protect listeners' interests by focusing on prohibitions against speakers' lies and misrepresentations,[395] especially when the strong speakers are the commercial actors that aim to influence consumers.[396] Regulating the lies of strong speakers and imposing honesty standards is important because lies are a powerful means of manipulation. They advance the liar's autonomy at the expense of the listener's interest to receive accurate information that enlightens decision-making.[397] Similar to lies, non-disclosures misrepresent the context surrounding the transaction. Non-disclosures threaten the consumer's interests while enhancing corporate interests. Non-disclosure maintains a façade of choice, yet it may sway decision-making.[398]

The concept of manipulation relates to hidden undisclosed factors that in fact constitute misrepresentation.[399] However, transparency does not justify manipulation.[400] Warning that a video contains subliminal advertising does not render the advertisement acceptable.[401] Moreover, it is not entirely clear what transparency means.[402] Despite this, conducting a cost-benefit analysis regarding disclosures,[403] outlining specific *ex ante* obligations not to lie regarding

---

394 Norton, *supra* note 47, at 441–42.

395 *See id.* at 451.

396 *See id*. at 458.

397 *See id*. at 451

398 *See id.* at 453.

399 *See* SUNSTEIN: THE ETHICS OF INFLUENCE, *supra* note 256, at 108 (a survey found that transparent nudges are less objectionable); Cass R. Sunstein, et al., *Trusting Nudges? Lessons from an International Survey* (2018), [https://perma.cc/3PK4-J64P]; Becher & Feldman, *supra* note 197, at 463 (proposing a broad conception of misleading information: "the definition of misleading or deceptive practices should be revisited and revised").

400 *See* SUNSTEIN, *supra* note 256, at 104.

401 *See id.*, at 23; *see also* GEORGE LOEWENSTEIN ET AL., WARNING: YOU ARE ABOUT TO BE NUDGED 1, 3 (2014) (describing how transparency does not always fulfill its goals).

402 SUNSTEIN, *supra* note 256, at 102 (explaining that is it is unclear what transparency should be about: the actions of the manipulator, the aspects of the situation, or something else).

403 Richard Craswell, *Taking Information Seriously: Misrepresentation and Nondisclosure in Contract Law and Elsewhere,* 92 VA. L. REV. 565, 566 (2006) (explaining that the question of which information should be disclosed and how requires balancing cost-benefit analysis).

the product's attributes and mandating specific disclosures can lead companies to act with material transparency and mitigate misrepresentation.

B. Lies and Nondisclosure: An Overview of Current Regulation

The regulation of lies and non-disclosures rests on the junction of a few areas of law: defamation law, FTC consumer protection regulation, and special regulations on advertising and endorsements.

First, defamation law can be a tool for combating false statements about competing brands that tarnish their reputations. Yet, while this may be a suitable tool for infringements by competing brands, it may not suit individuals who have been manipulated by false information. Moreover, defamation law is useful only with regard to negative information on brands, and not for false information endorsing a product.

Second, the FTC authorizes policing "unfair or deceptive acts or practices in or affecting commerce."[404] This regulation applies not only to traditional media, but also extends to the internet.[405] The FTC can initiate an interrogation or respond to individual consumer complaints,[406] or issue a policy statement on deception explaining that the case in question involves omission or other practices that are likely to mislead consumers.[407] The act or practice needs only to have the capacity to mislead in order to be deemed deceptive.[408] Intent to deceive is not necessary and the FTC need not show actual

---

404 *See* 15 U.S.C. § 45 (a)(1); Zarsky, *supra* note 24, at 186; Sprague & Wells, *supra* note 252, at 424–30.

405 FED. TRADE COMM'N, INFORMATION ABOUT ONLINE ADVERTISING (2000) ("The FTC has enforced and will continue enforcing its consumer protection laws online to ensure that products and services are described truthfully in online ads and that consumers get what they pay for.").

406 SUBMIT A CONSUMER COMPLAINT TO THE FTC, FED. TRADE COMM'N, https://www.ftc.gov/faq/consumer-protection/submit-consumer-complaint-ftc [https://perma.cc/Q687-JR24].

407 *See FTC Policy Statement on Deception*, FED. TRADE COMM'N (OCT. 14, 1983), appended to Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf [https://perma.cc/3TF9-GGRH].

408 Sprague & Wells, *supra* note 252, at 426 ("Since an act or practice need only have a tendency or capacity to mislead, the FTC need not find that consumers have actually been misled to declare an act or practice deceptive.").

damage.[409] Section 5 is vague and open to interpretation: the definitions therein are general and the question of what can mislead and what is "unfair" remains open.[410]

Third, although online ads are exempt from traditional media advertising disclosure requirements,[411] the FTC has outlined specific guides that apply to the internet in commercial contexts.[412] These guides focus on disclosure regarding endorsements by setting different standards for endorsements depending on the status and perceived expertise of the endorser. It includes special requirements for consumer endorsers and expert or celebrity endorsers.[413] An advertiser is subject to liability for misleading statements made through a paid blogger's endorsement.[414] A paid blogger is also subject to liability for making misleading endorsements or failing to disclose clearly that he was paid for his services.[415] The guides aim

---

409 HOOFNAGLE, *supra* note 375, at 124; Bladow, *supra* note 238, at 1135; Sprague & Wells, *supra* note 252, at 426.

410 Waldman, *supra* note 376, at 781; HOOFNAGLE, *supra* note 375, at 130 (explaining that the FTC has broad power to prevent unfair trade).

411 In addition to general obligations of fairness under the FTC Act, television and radio are subject to FCC regulation (47 U.S.C. §§ 317, 507). *See also* BENKLER ET AL., *supra* note 42, at 368 (referring to political advertising: "online ads have been to this date exempt from the disclosure requirements that normally apply to television, radio, and print advertising."); Goodman, *supra* note 372, at 145 (proposing that regulation should be neutral to technology). *But see* HOOFNAGLE, *supra* note 380, at 267 (explaining that regulation that is neutral to technology in marketing raises problems because different technologies allow different harm).

412 *See* Guides Concerning the Use of Endorsements and Testimonials in Advertising, 16 C.F.R. pt. 255 (2009).

413 *Id.* ("Advertisers are subject to liability for false or unsubstantiated statements made through endorsements, or for failing to disclose material connections between themselves and their endorsers [*see* § 255.5]. Endorsers also may be liable for statements made in the course of their endorsements."); Bladow, *supra* note 238, at 1125; Sprague & Wells, *supra* note 252, at 428 (explaining that although the FTC Guides on Endorsements are not themselves statutory or regulatory authority, they outline and provide guidance on the FTC's position on endorsements.); PASQUALE, *supra*, note 240, at 110 ("There is a long line of US Federal Trade Commission guidance forbidding misleading advertising and false or missing indication of sponsorship."); Lamo & Calo, *supra* note 201, at 1015 ("The FTC requires celebrities and 'influencers' on social media to disclose material connections with a company when they endorse a product, such as the fact that the company is paying them.").

414 Sprague & Wells, *supra* note 252, at 426, 433

415 Sprague & Wells, *supra* note 252, at 433 (explaining that an advertiser can limit his potential liability by ensuring that the statements it makes are truthful, monitoring bloggers

to mitigate practices of stealth marketing.[416] Thus, failing to disclose a sponsorship underlying an endorsement may be a deceptive act in violation of the FTC Act.[417]

The 2009 guides caused confusion about how to make disclosures regarding endorsements.[418] In its March 2013 guide, *.com Disclosures*,[419] the FTC addresses how businesses can modify their practices to comport with fair advertising.[420] While *.com Disclosures* focuses on all advertising mediums, it provides specific recommendations regarding disclosures for advertisements on social media platforms.[421] Thus for example, the FTC announced that space-constrained advertisements on Twitter or other social media platforms are not immune from disclosure requirements and provides instructions on how to disclose material connections between advertisers and users,[422] regulating the manner of disclosure, its visibility and prominence.[423] The 2013 guide does not have the force

---

that were paid to promote its products and taking steps necessary to halt the continued publication of deceptive representations when they are discovered). The standard of "clearly and conspicuously" remains ambiguous. *See* Bladow, *supra* note 243, at 1136.

416 *See* Leah W. Feinman, *Celebrity Endorsements in Non-Traditional Advertising: How the FTC Regulations Fail to Keep up with the Kardashians*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 97, 102, 122 (2011).

417 Sprague & Wells, *supra* note 252, at 424–26 ("[T]o establish liability under Section 5 of the FTCA, the FTC must establish that (1) there was a representation; (2) the representation was likely to mislead customers acting reasonably under the circumstances, and (3) the representation was material."). *See, e.g.*, *In re* TrendMark., Inc., 126 F.T.C. 375, 378 (2001) (alleging TrendMark had engaged in deceptive acts or practices because it did not disclose that the endorsers were either independent distributors or spouses of independent distributers of the marketer's product).

418 *See* Shannon Byrne, *The Age of the Human Billboard: Endorsement Disclosures in New Millennia Media Marketing,* 10 J. BUS. & TECH. L. 392, 394 (2015).

419 *Disclosures: How to Make Effective Disclosures in Digital Advertising,* FED. TRADE COMM'N (2013), https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf [https://perma.cc/VDZ9-MJR2] [hereinafter *Effective Disclosures*].

420 Byrne, *supra* note 419, at 359.

421 *Id.* at 402.

422 *Effective Disclosures, supra* note 420, at 16 (explaining that in space constrained advertisements, it is sufficient to begin the post with "Ad").

423 Byrne, *supra* note 419, at 403. *See, e.g., Effective Disclosures, supra* note 420, at 4; *id.* at 10 (placing a disclosure where an individual would need to scroll in order to discover it is not a sufficient disclosure, and explaining that hyperlinks on a social media platform leading to a disclosure are generally insufficient); *id.* at 16 (requiring that the disclosure occur within each endorsement post in order for it not to be considered deceptive).

of law. However, non-compliance may lead to FTC enforcement actions for unfair or deceptive practice in violation of the FTC Act. There is an underlying legal duty for businesses to avoid deceptive advertising and the guide articulates such rules of conduct.[424] The guide focuses on endorsement and sponsorship in exchange for benefits,[425] and neglects to address other types of stealth marketing that distort the flow of information.

C. Taking Disclosure Seriously

Legislators are promoting specific disclosure obligations on social media in political contexts. A bill—the Honest Ads Act—strives to ban undisclosed "electioneering communications," including reporting requirements for "political advertising" and online platforms for political advertisements.[426]

In the age of data driven advertisement that hacks human consciousness without sufficient transparency, it is time to promote broader disclosure obligations on companies in commercial contexts as well. The obligations would not eliminate the influence of manipulation altogether, but they would mitigate some of its effects.

1. The Limitations of Disclosure and the Path Forward

Manipulation is the problem but can disclosure be the solution? Mandated disclosure is appealing because it does not interfere with the free market principle. The market works best when buyers are informed and disclosure informs them. Moreover, disclosure equips

---

424 Byrne, *supra* note 419, at 412.

425 *See* Janée N. Burkhalter et. al, *Clear, Conspicuous, and Concise: Disclosures and Twitter Word-of-Mouth*, 57 BUS. HORIZONS 319, 321–23 (2014).

426 *See* Honest Ads Act S.1989, H.R. 4077, 115th Cong. (1st Sess. 2017); BENKLER ET AL., *supra* note 42, at 368; Goodman & Wajert, *supra* note 48, at 1 (identifying the trigger for the bill as the Russian interference in the 2016 United States elections and the need to ensure that electioneering communities are not funded by foreign nationals.). A law of disclosure should focus on payment for the advertisement and avoid imposing broad requirements on intermediaries, otherwise courts might grant injunction, holding the law as unconstitutional. *See e.g.*, Washington Post v. McManus, No. 19-1132 (4th Cir. 2019) (holding Maryland's proposed law regarding political advertisements, Online Electioneering Transparency and Accountability Act, as unconstitutional); Venkat Balasubramani, *Maryland Disclosure Requirements for Online Political Ads Violates the First Amendment*–Washington Post v. McManus, TECH. & MKTG. L. BLOG (Dec. 18, 2019), bit.ly/35CdoBb [https://perma.cc/22KM-HCUX].

individual autonomy to make life-shaping decisions.[427] Furthermore, disclosure can affect the behavior of its providers as they care about their reputations.[428]

Yet, disclosure is no panacea and it has its limitations. In *More Than You Wanted to Know*, Omri Ben-Shahar & Carl E. Schneider survey studies which suggest that mandated disclosure often fails to improve decision-making.[429] First, most individuals are decision averse.[430] Therefore, they are unlikely to seek and study disclosures,[431] since reading and understanding disclosures has costs and takes time. The decision to avoid reading a disclosure statement can be rational because for some decisions the costs of doing so exceed the benefits. Moreover, disclosure does not always promote autonomy because people often prefer a different kind of autonomy, in which they decide how well to inform themselves.[432] Second, people find it difficult to understand disclosures that can require high levels of literacy.[433] Third, mandated full disclosure results in information overload.[434] Fourth, the way the choice architect frames the information shapes individual decision-making.[435] The limited rationality of individuals hinders them from using reflective thinking to make decisions.[436]

Because there are far too many transactional aspects, regulators cannot require disclosure on each and every aspect of a transaction.

---

427 *See* BEN-SHAHAR & SCHNEIDER, *supra* note 98, at 5 (reviewing the rationales behind mandated disclosure).

428 *See* SUNSTEIN, *supra* note 98, at 108.

429 BEN-SHAHAR & SCHNEIDER, *supra* note 98, at 42.

430 *Id.* at 61.

431 *Id*.

432 *Id.* at 74.

433 *Id.* at 80; *see also* Benoliel & Becher, *supra* note 98, at 2263.

434 BEN-SHAHAR & SCHNEIDER, *supra* note 98, at 101 ("When mandates are too detailed, dense, and demanding, discloses often won't read them carefully—or at all. If they read them, they struggle to understand, analyze, remember, and assimilate the avalanche of information. Disclosures can overburden the mind, both by offering too many options and by providing too much information about each option."); *see also* SUNSTEIN, *supra* note 430, at 85 ("[O]ne cannot help . . . by the impossibility that anyone could attend to even a fraction of the disclosures to which we are exposed.").

435 BEN-SHAHAR & SCHNEIDER, *supra* note 98, at 114 ("However insightful the psychological literature is, it cannot equip lawmakers to mandate or disclosers to design disclosures that will rescue mandated disclosure.").

436 *Id.* at 110.

Although disclosure allows for improved flow of information to help make an informed decision, it can also be costly by obscuring other information and aspects of the transaction that are more important. A cost-benefit analysis is required to assess which information should be disclosed and how.[437]

The idea that absolute disclosure is inefficient is at the base of contract law. The assumption behind the Second Restatement of Contracts is that disclosure should be relative, involving costs and tradeoffs.[438] According to the Restatement, non-disclosure can be equivalent to misrepresentation and can constitute grounds for nullifying a transaction where the undisclosed fact would have corrected a mistake "as to a basic assumption on which that [other] party is making the contract."[439]

Liability for nondisclosure can rest on the theory of misrepresentation; however, cost and benefit tradeoffs have the same importance whether the regime is based on misrepresentation or nondisclosure.[440] In designing disclosure obligations regulators should consider the following: If planning on mandating certain information for disclosure, is it worth the cost of such disclosure? Or will disclosing the information interfere with the effective communication of other useful information, or have other costs that exceed its benefits?" [441]

Indeed, overall disclosure has more costs than benefits. S*pecific* mandated disclosure however, should not be ruled out. The idea of specific disclosure is not new.[442] Yet questions remain regarding

---

437 Craswell, *supra* note 374, at 566.

438 Restatement (Second) of Contracts § 161(b) (1981).

439 Craswell, *supra* note 374, at 574 (referring to Restatement (Second) of Contracts § 161(b) (1981), there are no criteria in the Restatement for distinguishing "basic" assumptions from other, less basic ones). *Id.* at 586–89.

440 *Id.* at 612–14 ("[E]ven misrepresentation cases cannot be assessed without attending to the costs and benefits.").

441 *Id.* at 614.

442 *See* Helen L. Norton, *The Government's Manufacture of Doubt*, 16 FIRST AMEND. L. REV. 342, 363 (2018) ("Legislatures can enact statutory responses to the government's expressive manufacture of doubt requiring the government to *make certain affirmative disclosures* and to otherwise constrain its lies and misrepresentations, and enforcement officials can more vigorously enforce existing laws that prohibit government agencies from engaging in covert propaganda or that *require the government to make certain information public*.") (emphasis added).

how policymakers and regulators should articulate specific rules of conduct to avoid unfairness or deception in the context of digital manipulation.

The idea of manipulation relates to hidden undisclosed elements that create a misrepresentation of facts, or false context for decision-making.[443] Disclosure regarding each and every hidden element of manipulation is however, both over-inclusive and under-inclusive. It is over-inclusive because there are countless hidden aspects of manipulation and the costs of disclosing all of them exceed the benefits.[444] It is under-inclusive because it would not necessarily counter the impact of manipulation and could obscure valuable information on important elements of the transaction.[445] Regulators should address the cost and benefit tradeoffs. The following Part will outline specific disclosure obligations concerning manipulation and explain the benefits of such obligations.

2. More than Content: Reducing Lies and Misrepresentations through Specific Mandated Disclosure

Multidisciplinary research addresses three main contextual factors that influence the flow of information.[446] First, it identifies the message, its context and the way it is represented.[447] Second, it identifies the source of the message.[448] And third, it pinpoints the context

---

443 SUNSTEIN, *supra* note 256, at 102. In a related context, a survey found that transparent nudges are less objectionable. LOWENSTEIN ET AL., *supra* note 401, at 5. *See* SUNSTEIN, *supra* note 98, at 42–44.

444 On the need to assess the costs and benefits of disclosure see generally CASS R. SUNSTEIN: TOO MUCH INFORMATION, UNDERSTANDING WHAT YOU DON'T WANT TO KNOW.

445 *See* LOEWENSTEIN, ET AL., *supra* note 401, at 2; Berman, *supra* note 45 at 533–34 ("Scientific studies further show that the subconscious effect of the mere exposure effect cannot be undone with a disclaimer.").

446 *See* Michal Lavi, *Taking out of Context*, 31 HARV. J.L. & TECH. 145, 150 (2017) (reviewing the literature on the main factors that influence the flow of information).

447 *See* MALCOLM GLADWELL, THE TIPPING POINT: HOW LITTLE THINGS CAN MAKE A BIG DIFFERENCE 91 (2000).

448 *Id.* at 60–62 (referring to "mavens" on social networks that "exert an unequal amount of influence on the decisions of others). In contrast, this Article refers to funded messages and "bots" that enhance messages and influence listeners who might not know that the source has less authority to recommend than they think (believing that the message is honest and the publisher is human).

of the situation.[449] These contextual factors can have a greater impact on the flow of information than the content of the message itself. Drawing on this insight, this Part proposes to expand existing disclosure obligations and adjust them to manipulation in data driven markets.

a) The Message: Avoiding False or Misleading Advertisements

The first general obligation relates to the commercial message itself. Advertisers should provide true information on material attributes of the product and avoid misrepresentations. After all, it is clear that the law ought to deter advertisers from disseminating misleading advertisements containing false information on their products.[450] Companies should also avoid lies regarding actual demand for the product, obscure hidden costs, and lies about other consumers' activities.[451] Such obligations are not new; the law already regulates misrepresentations in general contract law[452] and advertisements.[453] Moreover, avoiding lies is the baseline of the FTC consumer protection regulations.[454] In this respect, the ideas presented here are not new.

b) Contextual Elements

i. The Context of the Message - Indicating that the Message is Paid/Commercial/Inauthentic

The second general obligation expands the requirement for "Clear and Conspicuous Disclosures in Online Advertisements."[455]

---

449 GLADWELL, *supra* note 448, at 158; Michal Lavi, *Content Providers' Secondary Liability: A Social Network Perspective*, 26 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 855, 889 (2016).

450 Craswell, *supra* note 374, at 623.

451 Luguri & Strahilevitz, *supra* note 85, at 90 (referring to these acts of sneaking and making situations seem urgent as dark patterns, yet the FTC Act already considers these dark patterns to be lies).

452 Craswell, *supra* note 374, at 606.

453 15 U.S.C. § 1125(a)(1) (prohibiting, for example, the sale of products under any false description or representation).

454 The FTC's baseline rules? Don't lie. *See supra* sources cited, *supra* note 381; Craswell, *supra* note 374, at 594–95.

455 *Disclosures: Information About Online Advertising, supra* note 406, at 4; *see also* Byrne, *supra* note 419, at 403.

Advertisers and private individuals who endorse for payment bear liability for nondisclosure.[456] In the age of targeted advertising algorithms, the obligation to identify and mark ads as such may also applies to the intermediary that operates tools for purchasing targeted ads for revenue. Companies already apply ad promotion policies; for example, according to Facebook's advertising policy, ads promoting branded content should be tagged.[457] Twitter allows promoting tweets and targets them to specific audiences for a fee. The tweets are marked as "promoted."[458]

Similarly, commercial messages that are inauthentic, such as those created by deep fake technology, should be tagged as such.[459] Otherwise, consumers are likely to believe that someone they know, or a celebrity endorsed a product, even though he did nothing of the sort. Tagging the message might mitigate the misleading effects of such technology.

ii. Situational Context: Targeting

Companies usually target commercial messages by using an algorithmic tool. Consequently, consumers receive personalized ads that target them according to their specific inherent or contextual attributes at the time of message delivery.[460] Consumers are not always aware that the message is personalized and have no knowledge of the reasons for targeting, as this is a hidden element of manipulation. For that reason, Professor Carissa Véliz even suggested stopping personalized ads altogether.[461] Such a proposal is overbroad,

---

[456] Luguri & Strahilevitz, *supra* note 85, at 90 (referring to the FTC forming a basis for violations of disguised ads); *see also* BENKLER ET AL., *supra* note 42, at 372–74 (highlighting consequences in the context of politics).

[457] *See Transparency Center: Policies*, FACEBOOK, www.facebook.com/policies/ads [https://perma.cc/7YZ5-VJC4].

[458] *See Quick Promote*, TWITTER, business.twitter.com/en/solutions/twitter-ads/quick-promote.html [https://perma.cc/Q5RF-DJPL].

[459] Chesney & Citron, *supra* note 232, at 1753; *see also* Richard L. Hasen, *Deep Fakes, Bots, and Siloed Justices: American Election Law in a Post-Truth World,* 64 ST. LOUIS U.L.J. 535, 553–54 (2020) ("When it comes to whether video or audio has been manipulated, there is an objective truth of the matter: a scientific comparison of original content with content posted online.").

[460] *See* discussion *infra* Section III.C.2. (targeting that is based on location, personality traits, emotional state and engagement and social relations).

[461] *See* VELIZ, *supra* note 3, at 144, 152.

and it raises First Amendment concerns.[462] Instead, informing consumers of certain aspects of the advertising algorithm may comparably impact how they perceive and experience the advertisement.[463] As such, the intermediary should disclose contextual aspects of the advertisement, beyond simply indicating that the message is funded or promotional. This idea has already been established in the related political context of the "Honest Ads Act,"[464] and should also be adopted for commercial setting of advertising. Mandated disclosure in the age of algorithmic advertising should allow users to understand why they are seeing certain advertisements. It should indicate the targeted audience of the advertisement and the reason for specific personalized targeting of the relevant individual.[465]

For example, an explanation for targeting a McDonalds' ad to a consumer might denote "location," or "target audience–individuals at the mall."[466] Intermediaries can increase the visibility of disclosure mechanisms; [467] they can design explanations that are placed at the end of the ad.[468] A better option might be marking the advertisement with an icon: "personalized advertisement" or "details on targeting." This solution would allow interested consumers to view the complete information by clicking on the icon, while less interested consumers would be left with general understanding that the message is personalized. This option would enable a balance between prominent disclosure and detailed disclosure, while avoiding

---

462 *See* Jack M. Balkin, *The First Amendment in the Second Gilded Age*, 66 BUFF. L. REV. 979, 1009 (2018).

463 ESLAMI ET AL, *supra* note 462. Hugh J. Watson et. al, Addressing the Growing Need for Algorithmic Transparency, in 45 COMMUNICATIONS OF THE ASSOCIATION FOR INFORMATION SYSTEMS 488 (2019) (addressing a related issue of transparency).

464 *See* Honest Ads Act, S. 1989, 115th Cong. § 1 (2017) (proposing obligations of detailed disclosure and transparency to the Federal Election Committee).

465 ESLAMI ET AL, *supra* note 462 ("[A]s more ads are tailored to users via algorithmic processes, advertisers should provide users with interpretable explanations about these processes. Advertisers also need to increase the visibility of such disclosure mechanisms as the current practices fail to do so.").

466 ESLAMI ET AL, *supra* note 462 ("A minority of advertiser statements were interpretable—they provided specific information about the data or the inferences an advertising algorithm used to target a particular ad to a user.").

467 *Id.*

468 *Id.*

information overload for consumers who are less interested in such disclosure.

iii. The Context of the Speaker: The Source of the Message

"On the Internet, nobody knows you're a bot."[469] This ambiguity creates new possibilities for communication stemming from the affordability of bots. The source of the message influences the magnitude listeners ascribe to it.[470] Companies can sway consumers by creating a false impression about the reputation of the speaker and impacting the credibility listeners ascribe to the message.[471] They can use social bots that are engineered to engage with humans in a social-like manner, exercising learning, communication and adaptive software capabilities.[472] By presenting human-like characteristics and behaving as authentic social actors, bots evoke emotional responses, leading consumers to trust the source of message (an algorithm, instead of a human speaker) and influencing their decision-making.[473] Yet, trust in the bot is sometimes based on a false misrepresentation that the bot is human.

Concealing the source of a message is a misrepresentation.[474] Identifying the source of the advertisement and indicating that the speaker is an algorithm would allow consumers to evaluate the relevancy of arguments they are hearing and grant the arguments the proper weight. In order to protect consumers from the assumption

---

469 Lamo & Calo, *supra* note 201, at 992.

470 *See* Sprague & Wells, *supra* note 252, at 429 (explaining that listeners tend to ascribe anonymous messages less credibility, while ascribing more credibility to messages that come from a "maven" on their social network relative to a regular social network connection); *see also* Lavi, *Taking Out of Context, supra* note 447; *cf.* Goodman, *supra* note 372. On the importance of the source of the message in political contexts, see Helen Norton, *At Least Thirteen Ways of Looking at Election Lies*, 71 OKLA. L. REV. 117, 131 (2018). *See also* Goodman, *supra* note 372, at 132.

471 Cohen, *supra* note 15, at 148 ("Massively intermediated, platform-based media infrastructures have reshaped the ways that narratives about reality, value, and reputation are crafted, circulated, and contested.").

472 Lamo & Calo, *supra* note 201, at 994 ("Some bots can, subject to caveats and constraints, pose as human beings, simulating a certain degree of interpersonal communication on a particular topic.").

473 *See id.*

474 *See* Norton, supra note 443, at 355 ("[L]ies and misrepresentations include those that conceal itself as the *source of a message* to improve its reception in situations where the public might otherwise doubt the government's credibility.") (emphasis added).

that they are interacting with a human, mandated disclosure should be established,[475] requiring an automated account that interacts online to indicate clearly that the account is a bot. Legislators have already recognized the importance of disclosure regarding bots. Recently, the California State Senate voted to adopt a bill making it unlawful for any person to use a bot without disclosure. The bill applies only to commercial bots and bots seeking to influence elections.[476] However, the U.S. Senate is considering a blanket disclosure requirement for bots.[477] The FTC has also recognized the threat that human-like artificial agents pose to consumers and has passed regulations against "robocalls," artificial agents that call consumers and may be erroneously perceived as human.[478]

Bot disclosure laws do not limit the volume or content of bot speech. They stipulate obligations to inform the audience about its origins.[479] The idea of outlining disclosure obligations regarding the source of the message is no different from the current regulation of endorsements, designed to mitigate the harm of misrepresentation.[480]

The proposed contextual disclosure obligations can mitigate the harm of manipulation, promote a culture of transparency,[481] and enhance welfare. Specific disclosure obligations would have more benefits than costs. For example, requiring bot users to disclose a

---

475 *See* PASQUALE, *supra* note 240, at 109 ("[L]aws should require every account to disclose whether it is operated by a person or a machine.").

476 *See* Cal. Leg. S.B. 1001 Sess. 2017–2018 (2018); *see also* Lamo & Calo*, supra* note 201, at 991; Ellen P. Goodman, *Digital Fidelity and Friction*, 21 NEV. L.J. 623, 634–35 (2021) ("It requires that any 'automated online ['bot'] account' engaging a Californian on a purchase or a vote must identify itself as a bot. Notably, the law makes clear that it 'does not impose a duty on service providers of online platforms.'").

477 *See id.; see also* S. 3127, 115th Cong. (2018).

478 *See* Lamo & Calo *supra* note 201, at 996 ("[The FTC] has won several lawsuits against companies with predatory robocall practices.")*; see also FTC Providing $4 Million in Full Refunds to People Tricked into Buying Bogus 'Extended Auto Warranties*,*'* FED. TRADE COMM'N (July 19, 2016), https://www.ftc.gov/news-events/news/press-releases/2016/07/ftc-providing-4-million-full-refunds-people-tricked-buying-bogus-extended-auto-warranties [https://perma.cc/5CZG-4SK5].

479 *See* Lamo & Calo, *supra* note 201, at 1009.

480 *See* discussion *supra* Part III.B.

481 *See* Richards & Hartzog, *supra* note 128, at 1019 ("[A]ds could not continue in their current form but might continue if they are pursued in a transparent and loyal manner.").

bot's artificial identity, is a specific disclosure that is not expected to be expensive. Such disclosures have benefits in reducing manipulation and fraud by artificial entities.[482] In order to mitigate the problem of information overload, companies should simplify disclosures, present them in visual formats and allow consumers to click on them to receive detailed information. Savvy readers, information aggregators and other intermediaries are likely to read such disclosures,[483] spread the word on "creepy" targeting practices on social media, shame the media giants that allowed it online and even reach traditional media.[484]

Spreading the word on "creepy" advertising practices would raise public awareness about them. Consequently, consumers would be better informed about subliminal practices and would improve their decision-making. Even if disclosure and transparency cannot completely counteract the influence of subliminal subversion on deliberative thinking,[485] the diffusion of knowledge about the contextual aspects of advertising could mitigate their impact and lead companies to reduce manipulative targeting.

D. Enforcement and Remedies

1. The FTC Enforcement Regime

The FTC Act authorizes policing "unfair or deceptive acts or practices in or affecting commerce."[486] The terms "deceptive" and "unfair" as used in Section 5 are open to interpretation. Yet, the proposed disclosure obligation would clarify that the FTC has the authority to address failure to disclose specific elements of online advertising as well as to *prevent* future violations of disclosure obligations. The FTC has extraordinary powers; it can, for instance, bring cases against individual companies or bring administrative

---

482 Matthew Hines, *I Smell a Bot*: *Cal. S.B. 1001*, 57 HOUS. L. REV. 405, 411 (2019).

483 *See* BEN-SHAHAR & SCHNEIDER, *supra* note 98, at 185–90 (referring to the role of intermediaries in understanding disclosures, scrutinizing it and allowing the public to comprehend it); *see also* Calo, *supra* note 31, at 1026.

484 *See* Tene & Polonetsky, *supra* note 19, at 61 (coining the word "creepy" regarding unexpected practices of data collection and usage, and this term can be used for unexpected contextual elements of advertising).

485 *See* LOEWENSTEIN ET AL., *supra* note 402, at 11–12.

486 Federal Trade Commission Act, 15 U.S.C. § 45(a).

complaints and actions in federal court.[487] The FTC exercises its enforcement discretion and priority setting strategically, and addresses enforcement on a case-by-case basis to maximize its limited resources.[488]

The investigatory authority that provides the basis for enforcement is very broad.[489] It empowers the FTC "[t]o gather and compile information concerning, and to investigate from time to time the organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce."[490] Investigations can start in response to consumer complaints to the Consumer Sentinel system,[491] businesses exposing the practices of competitors, members of Congress who often forward consumer complaints on to the FTC, or just the observations of staff attorneys as they interact with companies.[492] "The FTC may resolve a pending investigation by closing the investigation, seeking a consent order, or issuing a complaint."[493] The FTC and the violator may enter into a consent order before or after the FTC issues a complaint.[494] A consent order makes it possible to settle deception allegations, often without admitting liability, and waives rights to judicial review.[495]

---

487 HOOFNAGLE, *supra* note 375, at 98.

488 *See id.* at 100; *see also* Bladow, *supra* note 238, at 1141.

489 Bladow, *supra* note 238, at 1142.

490 Federal Trade Commission Act, 15 U.S.C. § 46(a); HOOFNAGLE *supra* note 375, at 103; Bladow, *supra* note 238, at 1142.

491 FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK, https://www.ftc.gov/enforcement/consumer-sentinel-network [https://perma.cc/2Z5B-HD4S] (last time visited Dec. 17, 2022); Lauryn Harris, *Too Little, Too Late: FTC Guidelines on Deceptive and Misleading Endorsements by Social Media Influencers*, 62 HOWARD L.J. 947, 965 (2018-2019) ("The main ways that investigations are initiated are through: 'consumer complaints made on the Consumer Sentinel System, competitors exposing each other, members of Congress, or from staff members observations.'").

492 *See* HOOFNAGLE, *supra* note 375, at 103.

493 Bladow, *supra* note 238, at 1142.

494 *See* Bladow, *supra* note 238, at 1143; *see also id.* at 1146 ("[T]he risk or actual issuance of an administrative complaint can incentivize an advertiser to enter a consent order consisting of a voluntary agreement to discontinue the alleged deceptive practices and take steps to prevent future violations.").

495 *See* Bladow*, supra* note 238, at 1142–43 (stating that each violation of a consent order can lead to a civil penalty of up to $40,000).

Following an investigation, the FTC can bring a case in federal court or in adjudicative proceedings before an administrative law judge.[496] To enforce any civil penalty or seek consumer redress, the FTC must pursue litigation in court.[497] Judicial enforcement is advantageous because "the court may award both prohibitory and monetary equitable relief in one step."[498] When the FTC issues a complaint and the advertiser contests the allegations, the parties may proceed with an administrative trial resulting in a judge's recommendation to enter a cease-and-desist order or dismissal of the complaint.[499] After a review of a cease and desist order is complete, the FTC may file a civil action in federal court against the advertiser to seek relief for consumers. Once the order is final, the FTC can hold a nonparty liable for committing a deceptive act in violation of the order.[500]

The FTC also has a plenty of opportunities to enhance voluntary compliance.[501] "The FTC collaborates with law enforcement agencies on organized internet surfs to identify deceptive advertising practices,"[502] and issues access letters. These warning letters clarify to individuals and companies that their advertisement practices are deceptive and provides an opportunity to voluntarily comply with the law.[503]

The FTC has great power, yet at present it does not monitor platforms in general.[504] In addition, it does not investigate every complaint and has discretion in prioritizing complaints.[505] Although the FTC focuses its enforcement efforts on media giants that operate advertisement algorithms and are top influencers, many violations

---

496 *See* HOOFNAGLE, *supra* note 375, at 109.

497 Bladow, *supra* note 238, at 1143.

498 *Id.* at 243 (noting that there are no formal factors for matter selection).

499 *See* HOOFNAGLE, *supra* note 375, at 109; *see also* Bladow, *supra* note 238, at 1143.

500 *See* Bladow, *supra* note 238, at 1143.

501 *See id.* at 1144.

502 Bladow, *id.* at 1144.

503 *See* HOOFNAGLE, *supra* note 375, at 105–06; *see also* Bladow, *supra* note 238, at 1144.

504 *See* Rory Van Loo, *The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance*, 75 VAND. L. REV. 1563, 1566 (2019) ("Most notably today, federal regulators do not regularly monitor [Amazon, Google, Facebook and other] companies that run platforms, defined as sites 'where interactions are materially and algorithmically intermediated.'").

505 *See id.* at 1571.

still remain uninvestigated, resulting in under-deterrence.[506] Another shortcoming of FTC enforcement is that individual complaints do not result in private benefits to consumers.[507] Consequently, there is less incentive for private individuals to complain unless the complaint is about a competitor. Thus, there is limited knowledge of violations of non-disclosure obligations. Individuals do not have a remedy for the infringement of individual autonomy, and for the economic harm caused by lost choices and the purchase of unwanted products.

2. Private Enforcement Remedy or Compensation for Infringement of Autonomy

The digital environment challenges traditional methods of protecting fundamental rights. Therefore, current law must address new risks and harm to dignity and autonomy,[508] especially when these rights have economic value and protecting them promotes welfare. The scope and velocity of manipulation targeting particular individuals justifies new remedies.

This Part aims to apply a remedy recently proposed by scholars in the context of autonomy violations, tailored to the legal field of consumer protection regulation.[509] Drawing on Parchamovsky and Stein,[510] and applying their insights on rights and autonomy, and

---

[506] *See* Wyne Unger, *Reclaiming Our Right to Privacy by Holding Tech Companies Accountable*, 27 RICH. J.L. & TECH. 1, 13 (2020-2021) ("The FTC is resource constrained; only 40 full-time FTC employees are dedicated to internet privacy and data security. Its limited resources force the FTC to target businesses that are substantially harming consumers and cases that have a high likelihood of success. Therefore, many companies and deceptive business practices go uninvestigated.").

[507] *See Consumer Rights*, VERMONT'S LEGAL HELP WEBSITE (June 7, 2022), https://vtlawhelp.org/consumer-rights [https://perma.cc/YBD3-XKG7] ("The FTC cannot resolve individual consumer complaints[.]").

[508] In the related context of the scope of the First Amendment right to record in light of dignitary interests, see Margot E. Kaminski, *Privacy and the Right to Record*, 97 B.U.L. REV. 167, 217 (2017) ("[T]he scope of the protectable right changes because the nature of the harm changes."). *See also* Michal Lavi*, The Good, The Bad, and the Ugly Behavior*, 40 CARDOZO L. REV. 2597, 2607 (2019) (proposing a new remedy of a right to be forgotten to the dissemination of shaming information that does not reach the level of a tort or criminal offense).

[509] *See* Parchomovsky & Stein, *supra* note 287, at 5.

[510] *See generally id.* (developing a remedial framework designed to address autonomy violations).

remedial framework, the following part proposes that consumers would be able to file private actions and class actions *for infringement of disclosure obligations* if they were exposed to misrepresentation and then bought the product. The remedy would be available without evidence of a direct causal link between failure to comply with the disclosure obligation and the decision to purchase the product. This would allow consumers to collect damages for the loss of decision-making options.[511] Implementing this proposal would incentivize individuals to complain and file actions. It would also deter companies from disobeying disclosure obligations, bridge the gap in FTC enforcement and enhance the credibility of commercial messages.

a) Conceptualizing Harm to Autonomy

Parchomovsky & Stein explain that autonomy is the foundation of rights and not an incidental feature.[512] It represents a second-order right: an individual's basic entitlement to choose whether, when and how to realize his first-order rights and to protect his choices against unwelcome interference by others.[513] The wrongdoer should therefore be obligated to compensate individuals for the erosion of their right to autonomy.[514] Compensation for infringement of autonomy can also be justified from an economic perspective because autonomy confers a valuable option to right-holders, allowing them to decide whether and when to exercise their right. Options are valuable assets; people can buy and sell them on markets and they are a standard feature in contractual arrangements.[515] When someone unlawfully deprives an option holder of their decision-making power, as represented by the option, the option-holder suffers a loss.[516]

The current approach to law on harm to autonomy is unprincipled in the United States. Courts ignore the option value of

---

511 *See id.* at 15 (expanding on the economic value of option).
512 *See id*. at 4.
513 *See id*. at 10.
514 *Id*. at 15.
515 *Id*.
516 *Id. See also* Pauline T. Kim, *Manipulating Opportunity*, 106 VA. L. REV. 867, 894 (2020).

autonomy[517] and in most cases, deny redress for intangible harm linked directly to the infringement of autonomy.[518] Ignoring the value of autonomy is the rule, except for sporadic exceptions, primarily in the fields of medical malpractice[519] and constitutional law, which entitle victims to compensation for violation of their rights, without tangible harm linked to the autonomy infringement.[520] Even in these exceptional cases, courts have not referred to the victims' autonomy interest when recognizing their right to redress.[521] Rather, courts have chosen to invoke questionable legal constructs, such as "presumed harm," or to grant nominal damages to victims and supplement the reward with punitive damages.[522]

Due to the value of options in the context of autonomy, the law should recognize infringement of autonomy as grounds for a legal action based on violation of the right to choose, resulting in the loss of option. Since options have economic value, the loss of option is in fact actual harm. A causal link should be drawn between violation of mandatory disclosure requirements and harm to autonomy, without requiring a causal link between the failure to disclose and tangible harm.

---

[517] *See* Moore v. Regents of U.C. 793 P.2d 479, 497 (Cal. 1990) (holding doctors' duty to obtain patients' informed consent to treatment obligated them to tell the patient about their research and economic interests in the patients' cells, and failure to do so vitiated any consent to the treatment; however, human cells cannot be subject to ownership claims); Parchomovsky & Stein, *supra* note 287, at 16 (explaining that the court ignored the option value of the patient's entitlement to prevent the doctors' use of his biomaterials, and therefore failed to understand the patient's autonomy right).

[518] *See e.g.*, Pichowicz v. Hoyt, No. Civ. 92-388-M, 2000 WL 1480445, at *1 (D.N.H. Feb. 11, 2000) (rejecting a claim for autonomy harm and a fear of cancer claim, because plaintiffs did not prove that low level contaminants in their well caused neurotoxic effects, meaning their fears were "unreasonable").

[519] The doctrine of informed consent in medical malpractice started as a softer version of the tort of battery and developed into part of negligence law. The battery doctrines focused on elements of physical touch while the negligence doctrine focused on infringement of physical wellbeing. The harm in such cases does not link directly to the autonomy infringement. *See e.g.*, Truman v. Thomas, 611 P.2d 902, 907 (Cal. 1980) (liability for failing to explain the implications of avoiding a pap smear examination); *see* Marjorie Maguire Shultz, *From Informed Consent to Patient Choice: A New Protected Interest*, 95 YALE L.J. 219, 220 (1985) (proposing the creation of a distinct and independently protected interest in patient autonomy).

[520] Parchomovsky & Stein, *supra* note 287, at 18.

[521] *See id.* at 19, 29; *see e.g* W.J.A. v. D.A., 43 A.3d 1148, 1154–59 (N.J. 2012).

[522] Parchomovsky & Stein, *supra* note 287, at 18.

b) Legal Redress for Harm to Autonomy

Compensation for infringement of autonomy should apply to consumer protection and provide protection for consumer autonomy.[523] Affording redress for harm to autonomy has already been recognized outside the United States in various contexts,[524] including consumer protection.[525] For example, in *Late Tawfiq Rabi and the Israel Consumer Council v. Tnuva Food Industries Ltd*., a class action was filed after Tnuva Food Industries misled consumers regarding the ingredients of milk.[526] The company added silicon to its milk, in violation of health regulations, and lied to the public about it.[527] Tnuva denied this practice when the daily newspaper "Ma'ariv" first exposed it. Despite a lack of evidence of any risk associated with drinking milk with the concentration of silicon Tnuva added, Justice Amiram Binyamini of the district court ordered Tnuva to pay NIS 55 million in compensation to consumers and plaintiffs, due to harm to autonomy, even though Tnuva's misrepresentation did not cause tangible harm.[528] Tnuva appealed to the Supreme Court of Israel. Court approved the lower court ruling regarding liability, yet reduced the amount of compensation.[529]

A similar legal redress for harm to autonomy might be feasible in the case of misrepresentation in advertisements in violation of mandated disclosure.[530] When companies violate disclosure obligations in advertisements, individuals who saw the advertisement and bought the product would have a cause of action for violation of

---

523 *See id.*

524 *See* CivA 2781/93 Daaka v. Carmel Hospital, 53(4) IsrSC 526 (1999) (Isr.) (recognizing an independent harm to autonomy in failure to disclose the risks of a surgery, even though the doctors were not negligent).

525 CivC (DC TA) 1372/95 Late Tawfiq Rabi and the Israel Consumer Council v. Tnuva (Oct. 7, 2008) (Isr.).

526 *Id.*

527 *See* Noam Sharvit, *Tnuva Discovers Cost of Silicon in Milk***,** GLOBES (Oct. 7, 2008, 6:18 PM), en.globes.co.il/en/article-1000388630 [https://perma.cc/P4BF-22G7]; *Tnuva Fined NIS 55M for Silicon in Milk*, JERUSALEM POST (Oct. 7, 2008, 1:48 PM), www.jpost.com/Israel/Tnuva-fined-NIS-55m-for-silicon-in-milk [https://perma.cc/3G3Y-JPDC].

528 *See* Late Tawfiq Rabi and the Israel Consumer Council, at ¶ 46–51.

529 CivA 6339/09, 7607/09 Tnuva Food Industries Ltd. v. Late Tawfiq Rabi and the Israel Consumer Council, IsrSC, ¶ 58 (Dec. 12, 2011) (Isr).

530 *See supra* Part III(C)(2).

autonomy. This redress is justified for their loss of choice, since their decision to choose is based on misrepresentation. A failure to disclose information might be uncovered by a savvy consumer, civil society organizations, consumer organizations, news organizations, or other entities.

Indeed, an independent cause of action for harm to autonomy raises administrative concerns. Such cause of action might overwhelm courts by dramatically increasing litigation. To accommodate this problem, Parchomovsky & Stein outlined a threshold for affording legal redress for harm to autonomy. First, the law should condition suits for autonomy violations on the defendant's infringement of the plaintiff's recognized legal right; second, suits would undergo a strict de-minimis scrutiny; third, double recovery would not be allowed in cases where the harm inflicted on the plaintiff's autonomy was subsumed in his physical or economic loss.[531]

According to this framework, Consumers exposed to commercial advertisements in violation of disclosure obligations who then purchased the product would meet the threshold for filing independent legal action against the advertiser and the social media intermediary based on violation of autonomy. At present, common law of misrepresentation torts requires the element of reliance on the misrepresentation.[532] Yet, because every state has a different consumer protection statute, states should modernize common law in the context of failure to disclose in light of the FTC interpretation[533] that does not relate to the actual result of a misleading practice but rather the likelihood to mislead.[534]

---

[531] Parchomovsky & Stein, *supra* note 287, at 35–36.

[532] See Emily Sherwin, *Nonmaterial Misrepresentation: Damages, Rescission, and the Possibility of Efficient Fraud*, 36 LOY. L.A.L. REV. 1017, 1020 (2003) ("All sources agree that to claim either damages or rescission for misrepresentation, the plaintiff must show 'justifiable reliance' on the defendant's representation.").

[533] *See* FED. TRADE COMM'N, FTC POLICY STATEMENT ON DECEPTION, Appended to Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984), bit.ly/2XJqTyX [https://perma.cc/3TF9-GGRH].

[534] *See* Jean Braucher, *Deception, Economic Loss and Mass-Market Customers: Consumer Protection Statutes as Persuasive Authority in the Common Law of Fraud*, 48 ARIZ. L REV. 813, 855 (2006) ("Because every state has a broad consumer protection statute, it is appropriate to view these statutes and interpretations of them as a powerfully persuasive body of law that can help to modernize the common law of fraud. The Federal Trade Commission's interpretations of its own powers are very influential in the

Such suits meet the de-minimis threshold. They are not trivial because the misrepresentation of companies in advertising manipulates consumers and cause them to lose valuable options.[535] Suits would be confined to cases where there is a violation of specific disclosure requirements and would not extend to every instance of manipulation. Furthermore, filing individual actions would spotlight the problem of misrepresentation and draw attention to the harm of manipulation, which violates the autonomy of many consumers. Class actions would enable the mitigation of this cumulative harm to a great number of consumers.

In cases of digital manipulation, it is difficult to file a suit for economic harm due to obstacles in proving the causal link between the manipulation and the decision to buy. Recovery of full economic harm is likely to be rare, but if a plaintiff can prove a causal link, and economic loss that subsumes harm to his autonomy, he would be able to recover only for the economic harm incurred by buying the product. In contrast, compensation for violation of autonomy in digital marketing should include a predetermined statutory reward.[536] In cases of severe violation, courts should have discretion to grant additional compensation on top of the statutory amount.[537] This cause of action would enable consumers to find redress. It would also serve as an incentive to file suits for violation of mandatory disclosure and promote deterrence and enforcement.

c) The Problem of Standing for Harm to Autonomy Due to Misrepresentations in Commerce

The standing requirement can be an impediment to cases involving harm resulting in data misuse, such as anxiety regarding the consequences of data breach and future harm. When plaintiffs file an action in federal court, they have to demonstrate that they have

interpretation of state consumer protection laws and could be a source of development of the common law.").

535 Parchomovsky & Stein, *supra* note 287, at 38–39 (referring to similar violations that result in disempowerment and explaining that they are not trivial).

536 The law includes statutory damages provisions that may apply to manipulation. *See* Parchomovsky & Stein, *supra* note 287, at 34–35 (proposing to allow courts discretion to alter the statutorily set, non-percentage-based amount, in those cases in which the plaintiff suffered no significant economic losses).

537 *See id*. at 39.

suffered harm sufficient to establish Article III standing.[538] In *Spokeo v. Robins*, a database misused information on Mr. Robins and described him inaccurately.[539] The Supreme Court's decision limited standing, noting that a "bare procedural violation" is not concrete enough to provide standing. *Spokeo* left lower courts divided over the question of standing.[540] Recently in *TransUnion LLC v. Ramirez*,[541] "the Supreme Court concluded that most plaintiffs lacked standing in the class action suit, which arose from errors in credit reports. Although the credit report errors led some plaintiffs to be mislabeled as terrorists, the Court found that these plaintiffs had not demonstrated that the errors caused concrete harm." Scholars have referred to the *Spokeo* and *Trans Union* standards as bad policy and propose to adopt an expansive interpretation of harm.[542] Similarly, other scholarship proposes that significant constitutional standing problems stem from federal law, and therefore propose to adopt private enforcement remedies only at the state level.[543] In the context of advertisement, there is however, another solution that can allow address the problem of standing. Developing an independent cause of action for harm to autonomy as proposed, would recognize the infringement of autonomy as actual harm due to the economic value of option. Such a cause of action would overcome the barrier of standing.

IV. Data Retention Regulation for the Sake of the Future

A. Engineering Humanity and the Future

While disclosure obligations can mitigate some of the effects of manipulation in commerce, the regulation of lies and

---

538 *See* Daniel J. Solove & Danielle Keats Citron*, Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 739 (2018).

539 *See* Spokeo, Inc. v. Robins, 136 U.S. 330, 333 (2016); Ormerod, *supra* note 9, at 1922.

540 *See* Ormerod*, supra* note 9, at 1923 (comparing Beck v. McDonald, 848 F.3d 262, 267 (4th Cir. 2017), and Beck v. Shulkin, 137 U.S. 2307, 2307 (2017) with Attias v. CareFirst, Inc., 865 F.3d 620, 622 (D.C. Cir. 2017)).

541 TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2210 (2021).

542 Solove & Citron, *supra* note 541, at 767 (advocating the recognition of anxiety harm as actual harm); *See also* Daniel J. Solove & Danielle Keats Citron, *Standing and Privacy Harms: A Critique of Transunion v. Ramirez*, 101 B.U.L. REV. 62, 62 (2021).

543 Ormerod, *supra* note 9, at 1920 (discussing data breach and information misuse).

misrepresentation is only part of the solution. Even if disclosure requirements successfully increase consumer awareness, and help consumers make better informed decisions, such requirements alone cannot fully counteract the long-term effect of surveillance capitalism in constraining the free flow of information and consumer choice.[544]

Take, for example, content personalization, a method by which corporations use algorithms to predict future conduct based on users' past behavior with the goal of influencing consumer choice. Disclosure requirements would not prevent corporations from employing this particularly concerning tactic. With personalization, even if one "clicks around" on many different pages, the world of links presented to the viewer will be limited by their prior conduct.[545] These targeted interventions, which seek to shape a consumer's future decisions in a way that amplifies conformance with prior choices, pose a clear threat to free will and democracy.[546]

One way to limit the thought-constraining effects of personalization, is to focus upstream of the active influencing stage by regulating the collection and retention of data.[547] For example, legislators could intervene by inserting a stage into the data lifecycle —the "right to be forgotten." Already part of the General Data Protection Regulation (GDPR), the privacy regulation in Europe,[548] such a regulation could limit future use of data beyond the purpose of collection,[549] which would reduce the extent to which individuals could be tied to their past transactions.

While the right conferred by the GDPR would help curb personalization, American law places a greater weight on free speech in the balance against privacy than European laws do, and the EU

---

544 FRISCHMANN & SELINGER, *supra* note 28, at 117.

545 *See, e.g.*, Chen, *supra* note 302 (deleting Facebook released the New York Times reporter from the shackles of his past activities).

546 ZUBOFF, *supra* note 4, at 52–54.

547 VELIZ, *supra* note 3, at 156.

548 *See* Council Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 65, 2016 O.J. (L 119) 1 [hereinafter GDPR].

549 Tsesis, *supra* note 7, at 603; VELIZ, *supra* note 3, at 17.

regulation might be too broad to withstand First Amendment constraints.[550] Nonetheless, adopting a "right to be forgotten" *on a limited scale* would have more benefits than costs.

B. The GDPR, its Global Influence on Personal Data and Internal U.S. Pressure

1. GDPR- Background

The GDPR came into effect on May 25, 2018.[551] It presents a model of *omnibus privacy*, applying to all personal data irrespective of the type of sector in which it was collected,[552] recognizing the protection of personal data of all "natural persons" as a fundamental right.[553]

The GDPR protects this right by regulating the processing and retention of data in ways that limit the ability of data controllers to manipulate data subjects.[554]

First, GDPR follows previous data protection directives and prohibits processing sensitive categories of personal data unless specific conditions apply such as explicit consent of the data subject.[555] The ECJ has interpreted this prohibition broadly, applying it not only to websites but also to search engines.[556]

---

550 Tsesis, *supra* note 7, at 593.

551 *Id.*

552 POSNER & KENNEALLY, *supra* note 70, at 13.

553 For the definitions of "data controllers and data subjects" see Art 4 (1), 4(7) to the GDPR, *supra* note 548, at art. 1.

554 *See* Regulation (EU) 2016/679 of the European Parliament and the Council of April 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

555 *See* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, art. 8, 1995 O.J. (L 281) 1 (describing special categories of data); *see also* GDPR, supra note 548, at arts. 9–10. (referring respectively to processing of special categories of personal data such as race, political opinion, information about health, etc., and to processing of personal data relating to criminal convictions and offenses).

556 *See* Case C-136/17, GC v. Commission Nationale de l'Informatique et des Libertés, ECLI:EU:C:2019:773, ¶ 34 (Sept. 24, 2019).

Second, GDPR outlines a norm of data minimization by restricting personal data processing to data "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."[557] Companies are required to inform users of new purposes for processing and must provide clear terms to obtain user *consent* for commercializing their private data and enable them to withdraw that consent.[558]

Third, GDPR "limits the duration of time for which commercial audiences can retain personally identifiable information."[559] Article 15 of the GDPR gives all data subjects a *right of access* to their personal data.[560] Companies that control the data must inform data subjects of their rights to rectify, to erase, and to lodge a complaint and allow the data subject to correct the inaccurate information.

Article 17 of the GDPR provides EU data subjects a *right to erasure ("right to be forgotten")*.[561] This important provision burdens the data controller with obligations to erase data that is no longer necessary in relation to the purpose for which it was collected or processed. "The data subject can choose when to withdraw consent for retention of his data".[562]

Individuals also have a *right to object to* data processing. Article 21 includes a specific right to object to profiling, at any time. If the

---

557 GDPR *supra* note 548, at art. 5.

558 GDPR, *supra* note 548, at arts. 6–7; Tsesis, *supra* note 7, at 596.

559 GDPR, *supra* note 548, at art. 5(e) (explaining that data should only be retained for as long as is required to achieve the purpose for which the data were collected and processed, unless they need to be retained "for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes"); *see also* Tsesis, *supra* note 7, at 594.

560 GDPR, *supra* note 548, at art. 15 ("Right of access by the data subject").

561 GDPR, *supra* note 548, art. 17. *See* Lilian Edwards & Michele Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You Are Looking For*, 16 DUKE L. & TECH. REV. 18, 67 (2017); Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMMC'N. TECH. L. 65, 90 (2019) ("Roughly summarized, a data subject has a right to erasure when he or she successfully exercises the right to object, when the personal data were unlawfully processed, should be erased because of a legal obligation, or are no longer necessary in relation to the processing purposes."); Robert C. Post, *Data Privacy and Dignitary Privacy: Google Spain, the Right to be Forgotten, and the Construction of the Public Sphere*, 67 DUKE L. J. 981, 981 (2018); Tsesis, *supra* note 7, at 602.

562 Tsesis, *supra* note 7, at 603.

purpose of data processing is direct marketing, the data subject has *an absolute right to object*.[563] Article 22 of the GDPR addresses automated decision-making and states that individuals "have the right not to be subject to a decision based solely on automated processing."[564] However, data processors can sidestep this requirement by inserting human intervention into the process (human in the loop).[565] Another important provision is Article 25 that addresses "data protection by design and default," building privacy-friendly systems, starting from the beginning of the process of design.[566] Accordingly, "controllers must, at the time systems are developed as well as at the time of actual processing, implement 'appropriate technical and organizational measures'" to protect the rights of data subjects. In particular, "data protection by design and default" is required so that only personal data necessary for processing are gathered.[567] Main applications of data protection by design are: the anonymization and pseudonymization of personal data, a data minimizations approach during processing and storing data, storage limitation, transparency regarding processing and limited access to personal data.[568]

---

563 GDPR, *supra* note 548, at art. 21; *see also* Sandra Wachter, *Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR*, 34 COMP. L. & SEC. REV., 436, 443 (2018) (explaining that "in all other cases data processing must stop, unless the data controller can demonstrate compelling legitimate interests that override the interests of the data subjects").

564 GDPR, *supra* note 548, at art. 22. This prohibition applies only when the decision is "based solely" on algorithmic decision-making. Edwards & Veale, *supra* note 561, at 45–6; Margot E. Kaminski, *The Right to Explanation, Explained*, 34 BERKELEY TECH. L.J. 189, 196 (2019).

565 *See* Kaminski, *supra* note 564. at 201–02 (explaining that for an automated decision to fall outside of Article 22, human involvement must be meaningful); Meg Leta Jones, *Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood*, 47 SOC. STUD. SCI. 216, 217 (2017); Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data,* 47 SETON HALL L. REV. 995, 1016 (2017); Edwards & Veale, *supra* note 565, at 51.

566 GDPR, *supra* note 548, at art. 25; Edwards & Veale, *supra* note 561, at 77 (explaining that by doing so, it recognizes that a "regulator cannot do everything by top down control, but controllers must themselves be involved in the design of less privacy-invasive systems.").

567 GDPR, *supra* note 548, at art. 25.

568 *See, e.g.*, Oliver Vettermann, *Self-Made Data Protection—Is it Enough? Prevention and After-care of Identity Theft*, 10 EUR. J.L. TECH. § 4.1 (2019).

The GDPR expands individuals' rights to their data. It can mitigate manipulation by focusing on the first and second links of the data cycle and limits data retention instead of focusing on the stage of influence. It has the potential to mitigate the effects of advertisements on the future of individuals and prevent the engineering of humanity by commercial companies.

2. GDPR Influences on U.S. Regulatory Framework

The GDPR protects the data of EU citizens only. However, its influence extends beyond the EU borders, applying to non-EU companies that offer goods or services to EU consumers. Thus, it can affect data protection in the U.S. Furthermore, the GDPR contains a threshold test for international transfers of personal data to states outside its territory and a legal basis for blocking data exports to nations that do not meet this standard.[569] The threshold of extraterritorial transmission is the "*adequacy*" of data protection in the foreign jurisdiction.[570] Instead of an adequacy determination, the EU and the U.S. have developed the Privacy Shield: a voluntary private sector compliance program.[571] This bilateral agreement presents a list of substantive EU principles for American companies to follow voluntarily.[572] Yet, it should be noted that the European Court of Justice (ECJ) in Luxembourg had recently struck down the privacy shield in *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems,*[573] determining that the Privacy Shield

---

[569] *See* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U.L. REV. 771, 783 (2019).

[570] *See* GDPR, *supra* note 548, at art. 45; Schwartz, *id.* at 785 ("In its Article 45, the GDPR requires that the Commission consider a long list of factors in assessing the adequacy of protection, including 'the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral . . . as well as the implementation of such legislation, data protection rules, professional rules and security measures.'").

[571] The Privacy Shield replaced the Safe Harbor agreement. In *Schrems v. Data Protection Commissioner*, the ECJ declared that the Safe Harbor was invalid. Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, ¶¶ 342–43 (Oct. 6, 2015). Following this decision, the U.S and the EU reached a new arrangement called the Privacy Shield.

[572] C-311/18, Data Prot. Comm'r v. Facebook Ir. & Schrems, ECLI:EU:C:2020:559, ¶¶ 198–200 (July 16, 2020); Schwartz, *supra* note 569 at 795.

[573] C-311/18, Data Prot. Comm'r v. Facebook Ir. & Schrems, ECLI:EU:C:2020:559, ¶ 301 (July 16, 2020). *See* Javier Espinoza & Siddharth Venkataramakrishnan, *US-EU Data*

agreement did not limit access to data by US authorities in a way that satisfies requirements that are "essentially equivalent" to EU law. The impact of the ruling is not yet clear, as the court ruled that thousands of corporations that rely on the Privacy Shield to move data easily between the two regions might continue to do so under individual legal agreements covering how data will be treated.[574]

In addition to the direct influence of the EU regulation on U.S. data protection practices, the GDPR might have a broader "Brussels Effect": a race to the top in data protection standards,[575] as "data globalization" catalyzes the development of data protection legislation in the U.S.[576] For example, the California Consumer Privacy Act of 2018 (CCPA) was enacted in January 2020.[577] This law applies to companies that do business in the State of California, collect consumers' personal information,[578] and determines the means and purposes of processing.[579] The law does not incorporate the GDPR in its entirety,[580] but does adopt some of its key features including a

Sharing Deal Privacy Shield Struck Down by European Court, FINANCIAL TIMES (July 16, 2020), www.ft.com/content/b7a713e0-fe7e-4893-927c-7e90a1dd56d9 [https://perma.cc/P2SM-PXWK].

574 Omer Tene, *The Show Must Go On*, PRIVACY PERSPS., iapp.org/news/a/the-show-must-go-on/ [https://perma.cc/L5TH-BSN8] (last visited Dec. 18, 2022); *see also* Victoria Neiazy, *Invalidation of the EU–US Privacy Shield: Impact on Data Protection and Data Security Regarding the Transfer of Personal Data to the United States*, 2 INT'L CYBERSECURITY. L. REV. 27, 28 (2021) ("The Privacy Shield is no longer a valid transfer basis. According to the CJEU companies can still base their transfer on standard contractual clauses (SCCs) or other transfer tools under Article 46 of the General Data Protection Regulation (GDPR), but will have to review in each case whether this is sufficient. If that is not the case, they need to apply additional supplementary measures.").

575 Michael L. Rustad & Thomas H. Koenig*, Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 365 (2019).

576 *See* Anupam Chander, et al., *Catalyzing Privacy Law,* 105 MINN. L. REV. 1733, 1737 (2021).

577 CAL. CIV. CODE § 1798.198(a); *see* ERIC GOLDMAN, INTERNET LAW CASES & MATERIALS 1 (2019); Rustad & Koenig, *supra* note 579, at 403 ("It gives consumers the right to ask companies to disclose what data they have collected on them; the right to demand that they not sell the data or share with third parties for business purposes; and the right to sue or fine companies that violate the law.").

578 CAL. CIVIL CODE § 1798.140(o).

579 GOLDMAN, *supra* note 577, at 2.

580 Rustad & Koenig, *supra* note 575, at 404 (explaining that the GDPR contains many provisions that are absent from the CCPA, including: requirements for lawful processing; data and storage limitations; appointment of data protection officers, local representatives, performing a data protection impact analysis and specific requirements of data processors).

principle of data minimization, a right to access, and a right to know about practices of data collection including a disclosure obligation on business data practices.[581] It also outlines the right to erasure[582] and a right to say no to data sales,[583] and creates a dedicated clause for data breaches.[584] The law is likely to encourage large U.S. companies to adopt California's regulations and revise their privacy policies for all states in order to avoid having conflicting privacy policies across multiple states.[585] Further, the law has already influenced at least fourteen states to pass or introduce similarly-styled data protection bills.[586]

Yet, while the GDPR and the "California effect"[587] have expanded privacy protections in the U.S., the scope of American data protection laws remains narrower than in Europe.[588] For example, U.S. law targets only specific industries,[589] and allows for-profit information providers to gather information on data subjects.[590] Given

---

581 GOLDMAN, *supra* note 577, at 3; CAL. CIVIL CODE §1798.100(a–b); 1798.115; 1798.110; 1798.140(d, y).

582 CAL. CIVIL CODE § 1798.105 ("A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.").

583 CAL. CIVIL CODE § 1798.120(a). *See* GOLDMAN, *supra* note 577, at 3; Rustad & Koenig, *supra* note 575, at 403.

584 CAL. CIVIL CODE § 1798.150.

585 Rustad & Koenig, *supra* note 575, at 405; Olivier Sylvain, *The Market for User Data,* 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1087, 1096 (2019) (explaining that the GDPR and CCPA are "good indications that policymakers today are adapting current laws to meet the challenges posed by today's networked information economy").

586 *See, e.g.*, 2021 Va. Acts 1392; *see generally* Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. (forthcoming 2023); Neil Richards & Woodrow Hartzog, *Privacy's Constitutional Moment and the Limits of Data Protection,* 61 B.C.L. REV. 1687, 1691 (2020).

587 Rustad & Koenig, *supra* note 575, at 405; Chander et. al., *supra* note 576, at 1742, 1744.

588 Chander et. al., *supra* note 576, at 1755–56 ("[T]he CCPA does not treat privacy as a human right in the way data protection laws like the GDPR do. It remains, in the American tradition, a transactional privacy law concerned with protecting consumers in their dealings with commercial entities. For this reason, the CCPA does not embrace several principles that have been at the core of constitutionally influenced European data protection law since long before the GDPR.").

589 HOOFNAGLE, *supra* note 375, at 210.

590 Tsesis, *supra* note 7, at 599 (explaining that the default for U.S. internet transactions is that if the data subject has not opted out of an online tracking service, then that natural person's data can be resold to third parties; by contrast, the EU GDPR requires the data

the differences between the two continents with respect to rights, culture, commitments, and regulatory appetites, it is unlikely that GDPR style regulations will be adopted in full in the U.S. Whereas the American system has no explicit constitutional right to privacy, the status of privacy as a fundamental right in Europe is very clear.[591] Moreover, in Europe the right to free of speech is subject to proportionality analysis—where it conflicts with another fundamental right such as the right to privacy or data protection, courts must balance the rights equally.[592]

By contrast, in the U.S. freedom of speech is not subject to proportionality. Thus, regulation similar to the GDPR would conflict with the extensive protection provided by the First Amendment to freedom of speech, especially the public's right to receive information.[593] Moreover, many privacy protection provisions allowing individuals to manage their own privacy impose an administrative burden, with countless tasks required to exercise control becoming endless rendering one's control illusory.[594]

---

subject to opt in; that is, to grant limited written consent before the internet intermediary can post the information).

[591] *See* Richards & Hartzog, *supra* note 590, at 1696; European Convention for the Protection of Human Rights and Fundamental Freedoms arts. 7–8, Nov. 4, 1950, 312 E.T.S. 5.

[592] *See* Neil Richards & Woodrow Hartzog, *Privacy's Constitutional Moment*, 61 B.C.L. REV. 1687, 1729–30 (2020) ("In Europe, free expression is safeguarded by Article 10 of the European Convention and Article 11 of the EU Charter. Like other European fundamental rights, these provisions are subject to proportionality analysis—where they conflict with another fundamental right such as the right to privacy or to data protection, courts must balance the rights on an equal footing. By contrast, in the United States, the fundamental right of free expression protected by the First Amendment is not subject to proportionality analysis.").

[593] *See* Richards & Hartzog, *supra* note 592, at 1696; Oreste Pollicino & Macro Bassini, *Free Speech, Defamation and the Limits to Freedom of Expression in the EU: A Comparative Analysis*, *in* RESEARCH HANDBOOK ON EU INTERNET LAW 508 (Andrej Savin & Jan Trzaskowski eds., 2014). Tsesis, *supra* note 7, at 599 (discussing listeners' right to access information).

[594] *See* Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 18 (2021).

3. Limitation on Data Retention to Mitigate Commercial Manipulation

The ability of firms to "indefinitely retain data and sell it to third parties, even without the data subject's unambiguous, free, and informed consent," allows comprehensive profiling and effective manipulation.[595] Yet, far-reaching and effective manipulation would not be possible without extensive data retention. The main problem is retention of individual data by commercial entities, which shackles a person to the information collected on him is that the data allows manipulation of future decisions. Thus, retention of data may infringe on future development. Regulating data retention and outlining a right to erasure is essential for the sake of the future. For starters, data subjects should have a right to request the erasure of their information from servers. But, to truly protect consumers from thought shaping, data use for commercial purposes should be limited to the original transaction for which it was provided. Data can be archived for non-commercial uses such as promoting health, but not for the purpose of commercial targeting of advertisements. Companies should not profile and target advertisements to consumers based on comprehensive accumulated data on consumers. Even if companies would not be prohibited from using data for commercial targeting of commercial advertisements, there should at least be limitations, such as timelines for data retention.[596] Thus, commercia targeting of advertisement would not be based on the full consumer's profile and his history of interactions, and the degree of potential manipulation would be reduced. Further, federal law should regulate internet intermediaries' retention of personal data.[597] Such regulation doesn't rely on individuals managing their own privacy but focuses on the architecture that structures the way information is

---

595 Tsesis, *supra* note 7, at 629

596 Tsesis, *supra* note 7, at 628 ("Without a regulation requiring internet firms to periodically purge their records, they retain details that are not only useful for commercial audiences but at times are also misleading, defamatory, harassing, propagandistic, and inciteful.").

597 Tsesis, *supra* note 13, at 1626 ("In an age of such immense private data retention, the U.S. should join Europe by adding consumer privacy regulations of the internet to better preserve natural persons' fundamental rights to dignity, autonomy, and privacy").

maintained. Therefore, it is more likely to mitigate manipulation.[598] This type of regulation would not only broaden consumer freedom but also expand the commercial offers consumers receive, to offers that are not based on their personal data and their future commercial and other opportunities.[599]

Policy makers in the U.S. are starting to realize the important of imposing limitations on data retention. Recently, the White House Office of Science and Technology Policy published a "Blueprint for an AI Bill of Rights"[600] that addresses inter alia the need for clear timelines for data retention.[601] Although this statement is not binding, it aims to strengthen data privacy and safety of systems, and it is one positive step forward that can allow to indirectly mitigate manipulation.

It should be noted that this proposal does not aim to solve the problem of undue influence entirely but rather to mitigate it. Data protection regimes focused solely on procedural limitations are blind to activities that erode the freedom to choose and the asymmetry of power between consumers and the companies that collect and utilize their information.[602] Thus, a more comprehensive regulatory framework must be developed.[603]

---

[598] Solove, *supra* note 598, at 6 ("Privacy regulation can be best strengthened by regulating in ways that do not rely on individuals managing their own privacy. Instead, privacy regulation should focus on regulating the architecture that structures the way information is used, maintained, and transferred.").

[599] On manipulation of opportunities in the context of discrimination, see Pauline T. Kim, *Manipulating Opportunity*, 106 VA. L. REV. 867, 867 (2020) (discussing how less available information has the potential to reduce discrimination).

[600] THE WHITE HOUSE, BLUEPRINT FOR AN AI BILL OF RIGHTS—MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE (Oct. 2022) https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf [https://perma.cc/MRS9-L96M]; for criticism on this statement see Keith E. Sonderling, Bradford J. Kelley & Lance Casimir, *The Promise and The Peril: Artificial Intelligence and Employment Discrimination,* 77 U. MIA. L. REV. 1, 41 (2022).

[601] *See* Sonderling, Kelley & Casimir, *supra* note 604, at 33 ("Clear timelines for data retention should be established, with data deleted as soon as possible in accordance with legal or policy-based limitations. Determined data retention timelines should be documented and justified.").

[602] Richards & Hartzog, *supra* note 592, at 1738.

[603] *Id.* at 1739–40 (arguing that all four focal points of privacy must be addressed if a governing framework for our human information is to be complete: 1) corporate matters;

V. Regulation of Lies and Data Retention: Freedom of Speech Perspective

Regulating lies, mandating specific disclosures, and curtailing data retention practices inherently places certain limits on freedom of speech. First, regulation is directed at intermediaries and advertisers. Arguably, intermediaries that target algorithmic advertisements are immune to liability under Section 230 of the Communications Decency Act of 1996 (the CDA).[604] Second, mandating disclosures, while not limiting their speech, compels companies to speak and can conflict with their First Amendment rights. Third, limitations on data retention also conflict with First Amendment protection. The following Part addresses these concerns.

A. Section 230 Immunity

Section 230 of the CDA is among the most important digital age protections of freedom of speech in the United States.[605] Section 230(c) states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[606] Through this legislation, Congress expressed its intent that online intermediaries should not be treated as publishers for material authored by third parties.[607] Courts have interpreted Section 230 broadly and have repeatedly shielded web enterprises from primary and secondary liability in a wide variety of claims.[608] It may be argued that advertising

---

2) trustworthy relationships; 3) data collection and processing; and 4) personal data's externalities).

604 47 U.S.C. § 230(c)(1).

605 *See* Eric Goldman, *Why Section 230 Is Better Than the First Amendment,* 95 NOTRE DAME L. REV. 33, 34 (2019); Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2313 (2014).

606 *See supra* note 608; Jeff Kosseff, *A Users' Guide to Section 230, and a Legislators' Guide to Amending it, or Not,* 22 BERKELEY TECH. L.J. 2, 11 (2022); Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J.L. & TECH. 253, 262 (2006); Vanessa S. Browne-Barbour, *Losing Their License to Libel: Revisiting § 230 Immunity*, 30 BERKELEY TECH. L.J. 1505, 1525 (2015).

607 *See* Anupan Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639, 651–52 (2014) (highlighting that Congress sought to promote self-regulation and freedom of speech, and foster the rise of vibrant internet enterprises).

608 *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) ("By its plain language, § 230 creates a federal immunity to *any* cause of action that would make service

algorithms spread information provided by other content providers (typically advertisers) and therefore intermediaries should be immune to liability for these algorithms. As a result, consumer lawsuits against intermediaries for manipulation in this context could be barred in the preliminary stages.

Conceived when the internet was in its infancy, absolute immunity from suit for intermediaries allows corporations operating in the digital domain to avoid responsibility for potentially reckless or knowing conduct that violates consumers' basic privacy expectations.[609] As the internet matures, this scheme needs to be refined.[610] Recent scholarship evaluates several new concepts of liability for twenty-first century intermediaries that could be employed.[611]

One proposed solution is to revise the CDA's immunity provision such that it is available to operators only when they behave reasonably to prevent illegal activity.[612]

---

providers liable for information originating with a third-party user of the service."). *See also* Ricci v. Teamsters Union Loc. 456, 781 F.3d 25, 27–28 (2d Cir. 2015); Dowbenko v. Google Inc., 582 F. App'x 801, 804–05 (11th Cir. 2014); GoDaddy.com, LLC v. Toups, 429 S.W.3d 752, 756 (Tex. App. 2014). *But see* MARY ANNE FRANKS, THE CULT OF THE CONSTITUTION Ch. 4 (2019); Danielle Keats Citron & Mary Anne Franks, *The Internet as a Speech Machine and Other Myths Confounding Section 230 Speech Reform*, 2020 U. CHI. LEGAL F. 45, 51–52 (2020), for criticism on the creation of "two-track system of liability for offline and online" see Mary Anne Franks, *Reforming Section 230 and Platform Liability*, STAN. CYBER POL'Y CTR. (Jan. 27, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4213840 [https://perma.cc/74HD-E8BZ].

609 Balkin, *The Fiduciary Model of Privacy*, *supra* note 9, at 32 ("Section 230 holds companies harmless for a wide variety of wrongs that occur on their platforms."); *id*. at 33 (arguing that instead of focusing solely on content moderation, legislative proposals to narrow section 230's immunity "should aim at deeper sources of digital power. It should ask digital companies to reshape their business models and reduce the incentives toward manipulation.").

610 *See generally* Olivier Sylvain, *Intermediary Design Duties*, 50 CONN. L. REV. 203 (2018); Michal Lavi, *Do Platforms Kill?* 43 HARV. J.L & PUB. POL'Y 477 (2020).

611 *See* Tsesis, *supra* note 13, at 1624.

612 *See* Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break Denying Bad Samaritans § 230 Immunity*, FORDHAM L. REV. 401, 420 (2017); *see also* FRANKS, *supra* note 608, at 169 (advocating distributors knowledge-based liability for intermediaries).

Another proposal is to amend Section 230 and apply the immunity only on speech and not on mere marketplace activities such as connecting sellers and buyers and other trade practices.[613]

A third proposal, recently offered by Justice Against Malicious Algorithms Act (JAMA), narrows down Section 230 to exempt certain uses of technology,[614] specifically algorithmic amplification. This proposal aims to hold social media platforms accountable for their algorithmic amplification of harmful content, when such amplification is employed knowingly or recklessly to recommend content that causes material harm.[615] Further, JAMA eliminates Section 230 immunity for making a personalized recommendation of information that materially contributes to a physical or severe emotional injury.[616]

Such a policy could reduce algorithmic manipulation, however the language in the bill is too vague as to what content and conduct would "materially contribute to a physical or severe emotional injury."[617] In fact, this standard strips intermediary immunity for "any cause of action that recognizes physical or emotional injury–which is virtually all causes of action,"[618] This include protected speech, raising First Amendment concerns.[619] Such a standard impairs

---

[613] *See* Keats Citron & Franks, *supra* note 608, at 52; *see also* id. at 59 ("Intermediaries invoking Section 230's protections implicitly characterize the acts or omissions at issue as speech, and courts frequently allow them to do so without challenge. When 'courts routinely interpret Section 230 to immunize all claims based on third-party content'—including civil rights violations; 'negligence; deceptive trade practices, unfair competition, and false advertising; the common law privacy torts; tortious interference with contract or business relations; intentional infliction of emotional distress; and dozens of other legal doctrines'—they go far beyond existing First Amendment doctrine, and grant online intermediaries an unearned advantage over offline intermediaries.")

[614] *See* Justice Against Malicious Algorithms Act, H.R. 5596, 117th Cong. § 2(a) (2021).

[615] *See* Eric Goldman, *There is No Bottom When it Comes to Section 230 Reform Proposals (Comments on the Justice Against Malicious Algorithms Act)*, TECH. MKTG. L. BLOG (Oct. 18, 2021), https://blog.ericgoldman.org/archives/2021/10/there-is-no-bottom-when-it-comes-to-section-230-reform-proposals-comments-on-the-justice-against-malicious-algorithms-act.htm [https://perma.cc/59QJ-3LYN].

[616] *See* Justice Against Malicious Algorithms Act, H.R. 5596, 117th Cong. § 2(a) (2021).

[617] *Id.*

[618] *Id.*

[619] Daphne Keller, *One Law, Six Hurdles: Congress's First Attempt to Regulate Speech Amplification in PADAA,* CIS BLOG (Feb. 1, 2021), https://cyberlaw.stanford.edu/blog/2021/02/one-law-six-hurdles-congresss-first-attempt-

intermediary advertisement-based business models. What's more, it applies not only to targeting of commercial third-party ads but also to personalized recommendation on content and undermines intermediaries' business model altogether. Restrictions on personal recommendations can stifle beneficial recommendations and hamper free expression.[620]

Another, non-legislative, approach is to allow courts and regulators to rediscover the boundaries of immunity without a legislative change, and formulate an exception to the overall immunity.[621] Under this policy change, intermediaries, including communications platforms such as Facebook and Twitter, would not be treated as passive conduits for functions beyond content moderation. Courts could then rethink the scope of immunity in a way that matches the oversized effect intermediaries have on user conduct, while being attentive to intermediary design.[622] Such a policy change would likely impact the broader digital advertising market.

The argument for not applying the immunity on algorithmic design and targeting is that in this capacity, intermediaries deploy special tools to target advertisements, selecting advertisements for publication to specific users in specific contexts. Such sophisticated techniques that are way beyond moderation, fundamentally alter the user's experience of the message: influencing their interpretation, and increasing the magnitude they ascribe to it.[623]

Under this reading of Section 230, intermediaries that target advertisements can be held "responsible" at least "in part" for creating

---

regulate-speech-amplification-padaa [https://perma.cc/6BQ9-MWQP] (referring to hurdles of the Congress to regulate Amplification of speech in a previous bill).

620 Joe Mulin, *Lawmakers Choose the Wrong Path, Again, With New Anti-Algorithm Bill*, EFF (Nov. 11, 2021) ("Personalized recommendations happen a lot in the online world because they're useful to users. Users who have seen a good article, watched an interesting video, or shown interest in a product or service are often interested in other, similar things.").

621 *See generally* Michal Lavi, *Targeting Exceptions*, 32 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 65 (2021).

622 *See* Sylvain, *supra* note 610, at 218 ("Many of the most successful internet companies, moreover, design their applications to collect, analyze, sort, reconfigure, and repurpose user data for their own commercial reasons, unrelated to the original interest in publishing material or connecting users. These developments belie any suggestion that online intermediaries are merely conduits of user information anymore.").

623 *See* Lavi, *supra* note 443, at 153.

or developing defamatory content, and should not enjoy immunity.[624] Thus, lawsuits on personalized targeting without disclosure of the contextual elements of the advertisement, or for failing to erase consumer data after the transaction has been completed, would not be barred in preliminary stages. Some courts have already begun to apply a narrower interpretation of the immunity, recognizing the changing role of intermediaries,[625]and that the relevant claim does not treat the platform as the publisher or speaker of third-party content.[626]

Due to the increasingly manipulative impact of intermediaries on decision-making and the substantial harm they cause, a narrower interpretation of Section 230 is expected to be adopted.[627]). It should

---

[624] *See* Sylvain, *supra* note 610, at 272; Catherine Tremble*, Wild Westworld: Section 230 of the CDA and Social Network's Use of Machine Learning Algorithms,* 86 FORDHAM L. REV. 825, 866 (2017); JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET 188 (2019) ("As platforms increasingly develop more sophisticated algorithmic based technology to process user data it remains to see whether courts will conclude that they are responsible for the development of illegal content. For example, if a social media site allows companies to target their job advertisements to users under forty could the site be liable for developing ads that violate employment discrimination law? . . . [S]uch liability is possible though far from certain"); Lavi, *supra* note 610. *See also* Force v. Facebook, Inc., 2019 WL 3432818 (2d Cir. July 31, 2019), dissent ("When a plaintiff brings a claim that is based not on the content of the information shown but rather on the connections Facebook's algorithms make between individuals, the CDA does not and should not bar relief").

[625] *See* Jeff Kosseff, *A Users' Guide to Section 230, and a Legislators' Guide to Amending it, or Not,* 22 BERKELEY TECH. L.J. 22 (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3905347 [https://perma.cc/X8CP-UB2K]; Fair Housing Council v. Roommates.com, LLC, 489 F.3d 921, 929 (9th Cir. 2007), *rev'd en banc*, 521 F.3d 1157 (9th Cir. 2008). The Ninth Circuit declined to grant Roommates.com immunity. The court held that the intermediary is an information content provider with respect to the illegal questions on the site. This decision turned the developer into something more than just a "passive transmitter" of information.

[626] *See* Kosseff, *supra* note 629, at 21. *See e,g.*, Lemmon v. Snap, Inc., 995 F.3d 1085, 1088 (9th Cir. 2021); Loomis v. Amazon.com LLC, 2021 WL 1608878 (Cal. App. Ct. Apr. 26, 2021); Bolger v Amazon.com, Inc., 2020 WL 4692387 (Cal. App. Ct. Aug. 13, 2020); *see also* Harrington v. Airbnb, Inc., 3:17-cv-00558-YY (D. Or. Oct. 30, 2018); *see e.g.*, HomeAway.com v. City of Santa Monica, 918 F.3d 676, 682 (9th Cir. 2019) (finding liability arose from facilitating unlicensed booking transactions because a local regulation did not require the platforms to monitor third-party content or to remove it, it does not treat them as publishers, and thereby falls outside the preemptive scope of Section 230); KOSSEFF, *supra* note 628, at 166.

[627] *See* Jack M. Balkin, *How to Regulate (and Not Regulate) Social Media*, 1 J. FREE SPEECH L. 71, 94 (2021) (explaining that narrowing immunity in such cases will not lead

be noted that recently, the U.S. Supreme Court agreed to hear a case over the interpretation of Section 230. The case involves the argument that "international technology companies no longer shirk responsibility for online terrorist content."[628]

B. Regulating Lies and Data Retention: First Amendment Analysis

Freedom of speech enjoys stronger protections in the United States than in other Western democracies.[629] For example, the "right to record" can protect data collection,[630] and raw data may enjoy First Amendment protections.[631] In addition, algorithmic targeting constitutes "machine speech" which many scholars believe is included in freedom of speech,[632] especially regarding replicant

---

to disproportionate collateral censorship because intermediaries solicit advertisements for profit and that is how they make most of their money; they will still have an incentive to run ads even if the immunity is narrowed).

[628] *See* Ariel Kahana, *Israeli NGO Gets U.S. Supreme Court Nod in Bid to Hold Social Media Accountable for Terror*, ISRAEL HAYOM, https://www.israel-hayom.com/2022/10/09/israeli-group-gets-supreme-court-nod-in-bid-to-hold-social-media-accountable-for-terrorism/ (Oct. 10, 2022*); Ex-Israeli Intel Officials to SCOTUS: Social Media Platforms Aid, Abet Terrorism*, JERUSALEM POST, https://www.jpost.com/arab-israeli-conflict/article-724586 (Dec. 12, 2022).

[629] *See* Pollicino & Bassini, *supra* note 597, at 514. *But see* MARY ANNE FRANKS, THE CULT OF THE CONSTITUTION 169 (2019) (arguing that legislators, courts and civil rights organizations have interpreted the First Amendment selectively, almost like religious fundamentalists, and in fact they have infringed on the right of minorities and less powerful populations to free speech, shifting even more power from vulnerable populations to powerful ones).

[630] *See* Margot E. Kaminski, *Privacy and the Right to Record*, 97 B.U. L. REV. 167, 237 (2017).

[631] *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 557 (2011); Jane Bambauer, *Is Data Speech*?, 66 STAN. L. REV. 57, 72 (2014) (explaining that the First Amendment can protect raw data as it promotes the creation of knowledge).

[632] *See* Tony M. Massaro, Helen Norton & Margot E. Kaminski, *Siri-ously 2.0, What Artificial Intelligence Reveals About the First Amendment*, 101 MINN. L. REV. 2481 (2017) (arguing that the basis for applying First Amendment protections to machine speech is the public's right to receive information). *See also* Julie E. Cohen, *Tailoring Election Regulation: The Platform is the Frame,* 4 GEO. L. TECH. REV. 641, 641 (2020) ("[A]lthough one might wonder whether the data-driven, algorithmic activities that enable and invite such manipulation ought to count as protected speech at all, the Court's emerging jurisprudence about the baseline coverage of constitutional protection for speech seems poised to sweep many such information processing activities within the First Amendment's ambit."). *But see* PASQUALE, *supra* note 240, at 109 ("Free speech protections are for

speech that targets advertising.[633] Courts and scholars have developed theories about why freedom of speech should receive special protection.[634] It promotes individual autonomy and self-fulfillment,[635] as well as the search for truth[636] in the free marketplace of ideas. It also promotes self-governance and democracy,[637] and enhances a democratic participatory culture. The digital age pushes freedom of speech to the forefront, raising old concerns regarding expression.[638] The right balance must be struck between the benefits of freedom of speech and protecting consumers from disproportionate harm to autonomy and welfare.

Considering the balance of rights involved, commercial speech is especially suitable for regulation. The rationale for regulating this type of speech does not focus on the speaker's right to speak, but rather on the audience's right to know.[639] Moreover, the setting of commercial speech presents inequalities of information and power sometimes relevant in First Amendment doctrine.[640] In the past, the Supreme Court treated commercial speech as a distinct category

---

people, and only secondarily (if at all) for software, algorithms, and artificial intelligence.").

633 *See* Lawrence Lessig, *The First Amendment Does Not Protect Replicants, in* SOCIAL MEDIA AND DEMOCRACY (Lee Bollinger & Geoffrey Stone, eds. forthcoming, 2022) (manuscript at 13), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3922565 [https://perma.cc/8ZD5-DB7L] ("[T]he replicant targeting the ads in Facebook's algorithm would have no presumptive constitutional protection.").

634 *See* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 10 (2015) (reviewing influential theories which lay out justifications for the right to free speech).

635 *See* Joseph Raz*, Free Expression and Personal Identification*, 11 OXFORD J. LEGAL STUD. 303, 311–16 (1991).

636 *See* JOHN STUART MILL, ON LIBERTY 27 (1869); JOHN MILTON, AREOPAGITICA: A SPEECH FOR THE LIBERTY OF UNLICENSED PRINTING 6 (Cambridge Univ. Press 1918) (1644).

637 *See* ALEXANDER MEIKLEJOHN, FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT 46 (Harper & Brothers eds., 1948).

638 *Id.*

639 *See* Norton, *supra* note 47, at 441; Felix T. Wu, *Commercial Speech Protection as Consumer Protection,* 90 COLO. L REV. 631, 631 (2019) ("[T]he Supreme Court has long said that 'the extension of First Amendment protection to commercial speech is justified principally by the value to consumers of the information such speech provides."); Zauderer v. Off. of Disciplinary Couns., 471 U.S. 626, 651 (1985).

640 *See* Norton, *supra* note 316, at 230–31.

falling outside of First Amendment protection.[641] Later, in *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, the Court determined that the First Amendment protects commercial speech but not to the same extent as noncommercial speech.[642] In the decades that followed, both the boundaries of commercial speech and the consequences of falling within that commercial speech category became uncertain.[643] In *Central Hudson Gas & Electric Corporation v. Public Service Commission of New York,* the Court attempted to create a clearer framework.[644] The Court held that a regulation that completely banned an electric utility company from advertising to promote the use of electricity violated the First Amendment.[645] The Court set a four-prong test for reviewing restrictions on commercial speech, as an intermediate scrutiny test.[646] To qualify for First Amendment protection, (1) the commercial speech must concern lawful activity and not be misleading; (2) the interest in a regulation restricting the speech must be substantial; (3) the restriction must directly advance the government's asserted interest; and (4) the restriction must not be more extensive than necessary to serve government interest.[647]

The cases following *Central Hudson* have gradually moved in the direction of stricter review of limits on commercial speech.[648] In recent years free speech priorities have shifted from political speech to commercial speech and from individuals to corporations.[649] In *Sorrell v. IMS Health Inc.*, a Vermont statute prohibited data mining of pharmaceutical prescription files and restricted the sale, disclosure and use of records that revealed the prescribing practices of doctors.[650] Pharmaceutical companies analyzed the data to influence

---

641 Wu, *supra* note 643, at 632; Valentine v. Chrestensen, 316 U.S. 52, 54 (1942).

642 Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 770–73 (1976).

643 Wu, *supra* note 643, at 632–33.

644 *See* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 566 (1980); Berman, *supra* note 45, at 506.

645 Berman, *supra* note 45, at 571–72.

646 *Id.* at 566.

647 *Id.*

648 Berman, *Manipulative Marketing, supra* note 45, at 509–12 (reviewing the gradual move toward stricter scrutiny).

649 *See* FRANKS, *supra* note 612, at 13.

650 Sorrell v. IMS Health, Inc., 564 U.S. 552, 557 (2011).

physicians to prescribe expensive medications.[651] The Supreme Court struck down the law on First Amendment grounds and held that these restrictions warranted heightened judicial scrutiny.[652] The Court reasoned that content-based regulation could not be justified solely on the grounds of "fear that people would make bad decisions if given truthful information."[653] Therefore, "the State may not seek to remove a popular but disfavored product from the marketplace by prohibiting truthful, non-misleading advertisements that contain impressive endorsements or catchy jingles.[654] That the State finds expression too persuasive does not permit it to quiet the speech or to burden its messengers."[655] The Supreme Court finally gave industry what it sought in earlier cases by rendering the *Central Hudson* test irrelevant.[656] Thus, in practice, commercial speech can be treated as fully protected.[657]

Regulators and courts should generally move back in the direction of intermediate scrutiny. They can do so by reinstituting the *Central Hudson* test for commercial speech, with special considerations for the context of manipulative digital marketing. The justification for extending First Amendment protection to commercial speech is based on the information value such speech provides to consumers.[658] The commercial speech doctrine thus protects

---

651 *Id.* at 558.

652 *See* Jane Bambauer, *Information Libertarianism*, 105 CAL. L. REV. 335, 361 (2017) ("This outcome is consistent with info-libertarianism."); Berman, *supra* note 45, at 513 ("The Supreme Court's commercial speech cases show a heightened level of scrutiny being applied over time.").

653 *See* Sorrell, 564 U.S. at 577; Kilovaty, *supra* note 132, at 500.

654 *See* Sorrell, 564 U.S. 577–78; Kilovaty, *supra* note 132, at 500; Zarsky*, supra* note 24, at 178.

655 *See* Sorrell, 564 U.S. at 577; Kilovaty, *supra* note 132, at 499; Zarsky*, supra* note 24, at 178.

656 Tamara R. Piety, *"A Necessary Cost of Freedom"? The Incoherence of Sorrell v. IMS*, 64 ALA. L. REV. 1, 4 (2012).

657 *See id. But see* Berman, *supra* note 45, at 513 ("[P]roviding strong protection for 'truthful, non-misleading advertisements,' the Court suggested in Sorrell that a lower standard should apply if the government were restricting commercial speech for a 'neutral' purpose aimed at "protecting consumers from 'commercial harms.'") (quoting Sorrell, 564 U.S. at 578–79 (2011)).

658 Wu, *supra* note 639, at 632–33.

consumers—the listeners of commercial speech.[659] The rationale for First Amendment protection of targeted advertising is then the assumption that advertisers will provide audiences with useful information that will contribute to the marketplace of ideas. However, targeted advertising does not always encourage thought and introspection. Rather, through selective repetition and exploitation of cognitive biases, which companies identify through algorithmic analyses, ads can elicit interest through social imagery without providing listeners with objective and informative facts about products.[660]

Advertisements can be false or misleading and undermine the assumptions behind consumer decisions. Manipulation by companies goes beyond the content itself. It targets specific vulnerabilities, personalizes influences, targets consumers' emotional state, senses, and emotions[661] and communicates with consumers through human-like social actors (bots) that take advantage of consumer trust. This non-informational marketing exploits consumers' cognitive weaknesses and biases.[662] Non-verbal manipulation can subvert deliberative thinking without transparency, undermine consumers' overall utility, and may be misleading and deceptive. This may be true even if the information provided is accurate.[663] Manipulative marketing collapses the informational paradigm and does not promote the right of audiences to know, [664] because a significant percentage of ads focus on conveying "a particular image" for example by using emotional advertisements, instead of information about the product.[665] It

---

659 *See* Zauderer v. Off. of Disciplinary Couns., 471 U.S. at 651 (1985); Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n. 447 U.S. at 561 (1980). Wu, *supra* note 639, at 631; Tsesis*, supra* note 12, at 1597 ("[S]upreme Court precedents in this area have repeatedly conceived the protection of audiences' access to information to be critical for making good commercial decisions and selecting between advertised products.").

660 Tsesis, *supra* note 7, at 1613.

661 For example, advertisements can target fear and anxiety. *See* Norton, *supra* note 316, at 224–27; Tsesis, *supra* note 7, at 1621; see also Lamo & Calo, supra note 201, at 994–97.

662 *See* Berman, *supra* note 45, at 522.

663 *See* Becher & Feldman, *supra* note 198, at 477.

664 Berman, *supra* note 45, at 516 ("the trend since the 1970s has been for advertising to rely more and more heavily on lifestyle associations and emotional appeals, rather than the conveyance of information about the product.").

665 *Id.* at 517.

lacks human consciousness and provides de minimis benefits to the marketplace of ideas,[666] frustrating listeners' interests by "seeking to covertly influence those listeners' choices to the speaker's advantage."[667]

A stricter scrutiny test in the context of digital commercial manipulation, therefore, does not promote freedom of speech but infringes on it.[668] In contrast, the *Central Hudson*, intermediate scrutiny test provides a workable analytical framework for evaluating necessary restrictions on manipulative marketing.[669] Such intermediate scrutiny ensures that the government can provide evidence that the speech at issue is indeed harmful and manipulative, and that the regulation is not overbroad.[670] The following subsections demonstrate that the proposed regulations would pass intermediate scrutiny.

1. Avoiding False Commercial Messages and Misrepresentation

The first proposal prohibits false or misleading advertisements.[671] Falsehoods are protected speech only in non-commercial settings.[672] However, in a commercial context the legal balances are different. "The First Amendment safeguards the public's demand for commercial speech" in order to evaluate products: "that information is only helpful when it is authentic and truthful".[673]

---

666 *See* Berman, *supra* note 45, at 504; *see* Tsesis, *supra* note 13, at 1597.

667 Norton, *supra* note 315, at 221.

668 *See* Tsesis, *supra* note 7, at 1597.

669 *See* Berman, *supra* note 45, at 541; *supra* note 551 and accompanying text.

670 Berman, *supra* note 45, at 541.

671 *See supra* Section III.C.2. This proposal relates to the content of advertisements.

672 *See* United States v. Alvarez, 567 U.S. 709, 718 (2012); Louis W. Tompros et al., *The Constitutionality of Criminalizing False Speech Made on Social Networking Sites in a Post-*Alvarez*, Social Media Obsessed World*, 31 HARV. J.L. & TECH. 65, 68–69 (2017) ("some lies spread on social media may be protected"). *But see* CASS R. SUNSTEIN, LIARS: FALSEHOODS AND FREE SPEECH IN AN AGE OF DECEPTION 48 (2021) ("[T]he plurality in *Alvarez* was myopic in focusing largely on established categories of cases, such as defamation, in which false statements of fact can sometimes be regulated or sanctioned. In the modern era, false statements falling short of libel are causing serious problems for individuals and society; if they cause such problems, there is a legitimate argument that they should be regulable.").

673 Tsesis, *supra* note 7, at 1598.

Therefore, false and misleading commercial speech should be seen as unprotected within First Amendment doctrine.[674]

Misleading speech fails the first prong of the *Central Hudson* test by misleading consumers. Under such circumstances, the Supreme Court finds that "[i]f the speech does not pass this preliminary threshold, then it is not protected by the First Amendment at all."[675] Thus, regulation for avoiding falsehoods in the commercial setting is in line with the First Amendment.[676]

2. Specific Disclosure Obligations of Contextual Elements for Advertisements

The second proposal focuses on disclosure of contextual aspects of advertisements.[677] At first glance, it would appear that requiring companies to disclose does not conflict with the First Amendment because it does not censor speech. Yet, a deeper analysis reveals it can conflict with free speech doctrine.[678] The First Amendment protects individuals against government actions that compel them to speak what they choose not to.[679] Disclosure obligations in advertisement may amount to compelled speech.

Still, commercial actors may be compelled to disclose certain information about their products, and the First Amendment allows for greater disclosure requirements.[680] The justification for such disclosure is that more information is generally good for consumers.[681] Mandated disclosure of accurate, factual, commercial information does not conflict with the core of First Amendment values but rather

---

674 See *id*.

675 *Id.* at 1611 (referring to City of Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 434 (1993)).

676 *See* Norton, *supra* note 47, at 444 (referring to inequality between users and companies vis a vis information and power); *see also id.* at 452.

677 *See supra* Section III.C.2.

678 *See* Lamo & Calo, *supra* note 201, at 1009.

679 *See* Wooley v. Maynard, 430 U.S. 705, 714 (1977); *see also* Goodman, *supra* note 377, at 133.

680 Zauderer v. Off. of Disciplinary Couns., 471 U.S. 626, 651 (1985) (holding that the state could require disclosures that are "reasonably related" to preventing consumer deception); Lamo & Calo, *supra* note 201, at 1010.

681 Lamo & Calo, *supra* note 201, at 1011.

contributes to the efficiency of the 'marketplace of ideas.'[682] For example, agency regulations may require commercial products to bear "the name and place of business of manufacturer, packer, or distributor."[683] The government cannot force commercial speakers to endorse ideas contrary to their own interests;[684] but the government can impose disclosure obligations that provide consumers with information.[685] Such regulation would not implicate particular viewpoints but merely require that advertisers disclose contextual aspects of advertisements. In the context of manipulation, without mandated disclosure the market would fail to produce information that enhances public welfare.[686]

A further First Amendment concern is that free-speech doctrine protects speakers' right to conceal their identity, particularly where a speaker chooses anonymity in order to express unpopular or dissenting ideas.[687] The right to anonymity is part of the freedom of speech because an identification requirement would tend to restrict the freedom to distribute information.[688] However, requiring disclosure that a message is commercial, and that the speaker is a bot, strikes a different balance between rights than requiring disclosure of a speaker's identity. On the one hand, requiring bots to identify themselves limits speech and impairs the audience's right to information, because platforms may automatically prohibit bot speech

---

682 *Id.*

683 *Id.* at 1010; 21 C.F.R. § 101.5 (2018); 21 C.F.R. § 201.1 (2018).

684 Lamo & Calo, *supra* note 201, at 1012; *see also* Goodman, *supra* note 372, at 136; *see also* Nat'l Inst. of Fam. & Life Advoc. v. Becerra, 138 S. Ct. 2361, 2366 (2018).

685 Omri Ben-Shahar & Carl E. Schneider, *The Futility of Cost-Benefit Analysis in Financial Disclosure Regulation*, 43 J. LEGAL STUD., S253, S254 (2014) ("Disclosure is lawmakers' favorite technique not only in financial regulation, but ubiquitously. Vast stretches of consumer-protection law mandate disclosures.").

686 *See* Goodman, *supra* note 372, at 137-38.

687 JEFF KOSSEFF, THE UNITED STATES OF ANONYMOUS 37–55 (2022).

688 *See* Talley v. Cal. 362 U.S. 60, 64 (1960) (striking down a municipal ordinance that prohibited the distribution of handbills that did not include the name and address of the person issuing them. The Court reasoned that "an identification requirement would tend to restrict freedom to distribute information and thereby freedom of expression."); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) (striking down an Ohio law prohibiting the distribution of campaign literature that did not contain the name and address of the person issuing it.); Lamo & Calo *supra* note 201, at 1023 ("[F]irst Amendment protects the right to speak and even litigate anonymously.").

altogether.[689] On the other hand, commercial bots can harm consumers by creating fake reviews,[690] the volume of which can increase their credibility and mislead consumers into making a sub-optimal purchase decision.

Indeed, the capacity of bots for harm does not justify blanket requirements of bot self-disclosure without reference to context.[691] Legislation should not arbitrarily limit a newly developing communication medium. However, as Madeline Lamo and Ryan Calo have proposed, regulation can be justified within specific contexts and supported by specific harm the government hopes to mitigate.[692] Commercial bots are different from political ones, as they involve messages that are not at the core of First Amendment protection. Interests in concealment do not counterbalance disclosure interests in transparency.[693] Moreover, in the context of the digital market, the potential of manipulation's harm is extensive. Avoiding disclosure may manipulate consumers to adopt false beliefs regarding the message, since the context and source are part of the message.[694] Therefore, given the importance of consumer protection in this commercial context, mandated disclosure is in line with First Amendment.[695]

3. Limitations on Data Retention

At first glance, data is more of a commodity than a type of speech, and therefore should find no protection under the First Amendment.[696] At the same time, it can be argued that data is in fact

---

689 *See* Lamo & Calo, *supra* note 201, at 1024.

690 Bots can endorse a brand or defame a competing brand through fake reviews. *See id.* at 997; Tsesis, *supra* note 13, at 1621–22 ("Bot messaging is rather a technical tool for exaggerating, generating such an overwhelming amount of false information to silence countervoices, and thereby confusing the public. Robotic messaging can be used to attack deliberative democracy's administrative tools.").

691 *See* Lamo & Calo, *supra* note 201, at 1026.

692 *See id.* at 1027.

693 *See* Goodman, *supra* note 371, at 135.

694 *See* Lavi, *supra* note 470, at 151.

695 *See* Lamo & Calo, *supra* note 201, at 1011.

696 *See* Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1169–73 (2005).

speech as it protects the right to create knowledge.[697] But even if data is speech, the value of speech is not absolute. With time, data may take on fewer aspects of free speech.[698]

Moreover, the marketplace of commerce is not the marketplace of ideas.[699] Commercial collection and analysis of data is not public opinion but rather a form of market behavior that uses speech.[700] First Amendment protection of the audience's access to ideas and experiences does not imply that commercial entities have any constitutional right to indefinitely retain and manipulate psychometric information on consumers.[701] To reflect this reality, regulation should be subject to intermediate scrutiny standards to review regulations governing how long firms can commercially retain and analyze individual information.

The interest in regulating the duration of data retention and storage is substantial. Such regulation is important for mitigating the damage caused by shackling individuals to their past decisions and infringing on their future development. Limitation on data retention applies in commercial purposes and is narrowly tailored to serve this interest.[702] Such limitations relate to time, place, and manner of data practice; thus, they are neutral to content, and pass the intermediate scrutiny test.[703]

The proposed regulation of lies, misrepresentation, and data retention is consistent with the First Amendment. Limits to data retention guarantee the long-term survival of a marketplace of ideas in

---

697 *See* Sorrell, 564 U.S. at 557 (prohibiting pharmaceutical companies from receiving and using prescription data to customize their advertising to doctors brought a First Amendment challenge. The majority opinion struck down the law, finding it unconstitutional); *see also* Bambauer, *supra* note 631, at 57.

698 *See* MEG LETA JONES, CTRL + Z: THE RIGHT TO BE FORGOTTEN 157 (2016) (explaining that data can be considered speech, but the scope of the First Amendment with regard to protecting data is not absolute).

699 Tsesis, *supra* note 7, at 1588 ("The marketplace of commerce is not the same thing as the marketplace of ideas.").

700 *See* Hirsch, *supra* note 320, at 502.

701 *See* Tsesis, *supra* note 7, at 1588; *see also* Lavi*, supra* note 614, at 516.

702 *See* Tsesis, *supra* note 7, at 1614.

703 *See id.* (noting that reasonable time, place, and manner restrictions can be made on the duration of data retention).

which individual listeners make fairly autonomous decisions without being shackled to their past trail of information.

Conclusion

> *If the digital future is to be our home, then it is we who must make it so. We will need to know. We will need to decide. We will need to decide who decides. This is our fight for a human future.*[704]

In the new order of surveillance capitalism, central intermediaries know everything about consumers. They modify their behavior and influence their decisions as if consumers were puppets in their hands. This type of deep influence cannot be reduced to known legal arenas such as antitrust or privacy.[705] Policy makers have yet to develop strategies to combat robust manipulation in digital markets that infringe on consumer autonomy, welfare and the democratic order.

This Article focuses on one consequence of surveillance capitalism: the problem of manipulation in digital markets. It argues that manipulation should be subject to legal regulation, and addresses the questions of when and how. It develops strategies to mitigate the harm of manipulation. First, the Article demonstrates how disruptive technologies at the service of companies have led to the development of new methods of influence on consumer decision making throughout the data lifecycle; starting with surveillance and collecting data on consumers, analyzing it and exploiting innovative methods to target vulnerabilities.

Afterwards, the Article defines manipulation and addresses the unique concerns it raises in the digital era. The Article then promotes the concept of liability while setting out limiting principles. It proposes a focus on lies and online disclosure obligations. Companies that present false information in advertisements or fail to disclose contextual aspects of commercial advertisements should be subject to administrative enforcement. Moreover, consumers who were

---

704 ZUBOFF, *supra* note 4, at 62.

705 *See id.* at 52–55.

exposed to commercial misrepresentation should be able to find redress in a new remedy of compensation for harm to autonomy.

This solution cannot mitigate the long-term effects of manipulation: the engineering of humanity by using data on the past activities of consumers and creating a loop that shackles consumers to their past decisions with no way out. To mitigate this effect, this Article proposes limitations on data retention for commercial purposes. Finally, this Article demonstrates that the proposed balance between freedom of speech and consumer protection is in line with First Amendment doctrine and can even promote freedom of speech.

This Article is not the final word on this topic. The proposed solutions can mitigate the harm of manipulation; yet the solution is incomplete. It focuses on specific disclosure obligations on existing technology, while new strategies of manipulation that subvert deliberative thinking are likely to develop. Moreover, it proposes limitations on the retention of data collected for commercial purposes; yet data can be collected in other contexts and used for manipulation. For example, health information can be collected to mitigate the risk for viruses. Yet, the same data can be used for commercial purposes, stigmatizing, and discrimination. These challenges and others deserve future exploration. Hopefully, future work will further adjust this framework for countering manipulation to issues outside of the commercial context.