LEGALLY COGNIZABLE MANIPULATION

Ido Kilovaty†

ABSTRACT

Swaths of personal and nonpersonal information collected online about Internet users are increasingly being used in sophisticated ways for online political manipulation. This represents a new trend in the exploitation of data, where instead of pursuing direct financial gain based on the face value of the data, actors engage in data analytics using advanced artificial intelligence technologies that allow them to more easily access individuals' cognition and future behavior. Although in recent years the concept of online manipulation has received some academic and policy attention, the desirable relationship between cybersecurity law and online manipulation is not yet fully explored. In other words, regulators and courts have yet to realize the importance of linking cybersecurity law to individual autonomy, privacy, and democracy.

This Article provides an account of the desirable relationship between cybersecurity law and other values, such as autonomy, privacy, and democracy, by looking at the phenomenon of online manipulation achieved through psychographic profiling. It argues that the volume, efficacy, and sophistication of present online manipulation techniques pose a considerable and immediate danger to autonomy, privacy, and democracy. Internet actors, political entities, and foreign adversaries carefully study the personality traits and vulnerabilities of Internet users and, increasingly, target each such user with an individually tailored stream of information or misinformation with the intent of exploiting the weaknesses of these individuals. This Article makes a broader argument about cybersecurity law and its narrow focus on identity theft and financial fraud. Primarily, this Article looks at data-breach notification law, a subset of cybersecurity law, as reflective of that limited scope. It argues that data-breach notification law could provide a much-needed backdrop for the challenges presented by online manipulation, while alleviating the sense of lawlessness engulfing current misuses of personal and nonpersonal data. At the heart of this Article is an inquiry into the expansion of dated notions of cybersecurity law.

DOI: https://doi.org/10.15779/Z38T727G4R

† Frederic Dorwart Endowed Assistant Professor of Law, University of Tulsa, College of Law; Cybersecurity Policy Fellow, New America; Visiting Faculty Fellow, Center for Global Legal Challenges, Yale Law School; Affiliated Fellow, Information Society Project, Yale Law School. I wish to personally thank Claudia Haupt, Andrea Matwyshyn, and Robert Spoo for their guidance and support, the members of the Berkeley Technology Law Journal for their meticulous and thorough work on this Article, the organizers and participants of the 2018 Northeast Privacy Workshop and Ohio State University Center for Ethics and Human Values COMPAS Conference on Targeting with Big Data for their helpful feedback. I'm indebted to the College of Law at the University of Tulsa for its generous summer research stipend to support this project.

Presently, cybersecurity law's narrow approach seeks to remedy materialized harms such as identity theft or fraud. This approach contravenes the purpose of cybersecurity law—to create legal norms protecting the confidentiality, integrity, and availability of computer systems and networks. If cybersecurity law seeks to protect individuals from the externalities of certain cyber risks, it needs to recognize emerging threats targeting computer systems and networks, and subsequently, individual autonomy, privacy, and democracy.

TABLE OF CONTENTS

I. INTRODUCTION

The landscape of data breaches and personal information misuse is changing. Malicious actors are constantly seeking more efficient, sophisticated, elusive, and low-risk methods of exploiting our data.[1] Surely, the traditional

1. This notion is directly tied to the "accepted wisdom" that in cyberspace, attackers always have the advantage and are constantly able to overcome new defense techniques. *See, e.g.*, David T. Fahrenkrug, *Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy*, *in* NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, 4TH INTERNATIONAL

form of data breaches is still taking place as it has been for the last two decades. Databases are being constantly hacked and their data exfiltrated, to subsequently be exploited or sold.[2] The proliferation of data breaches has created the perception, which became a slogan, that it is not a question of "if you will get breached" anymore, but rather "a question of when."[3] These financial-facing forms of data breaches, often resulting in identity thefts and fraud, are still taking place today.[4] Indeed, most litigation in that context is due to credit card information theft.[5]

Yet, recent scandals surrounding alleged digital interferences in elections and referendums throughout the world suggest that personal and nonpersonal information obtained in data breaches may facilitate a new form of harm. These scandals illustrate that perpetrators may use personal information not only for direct financial gain, as they did for more than two decades, but also for the largely unanticipated political manipulation and direct microtargeting of the data subjects.[6] This poses the question: what is the role of cybersecurity law today, given these new threats? Do the governing definitions, scopes, and conceptions of cybersecurity law comport with today's threats?[7] This Article

CONFERENCE ON CYBER CONFLICT. PROCEEDINGS 2012 197 (C. Czosseck et al. eds., 2012).

2. *See* Lily Hay Newman, *If You Want to Stop Big Data Breaches, Start with Databases*, WIRED (Mar. 29, 2017), https://www.wired.com/2017/03/want-stop-big-data-breaches-start-databases/ [perma.cc/6MHD-BYSZ] (noting that the increase in data breaches is tied to the proliferation of databases containing "tempting troves of customer and financial data" with often outdated and weak security).

3. David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935, 936 (2016).

4. *See* George Ashenmacher, *Indignity: Redefining the Harm Caused by Data Breaches*, 51 WAKE FOREST L. REV. 1, 4 (2016) ("These breaches cause tangible, financial harms to the individual. Identity theft and accompanying fraud constitute a growing type of criminal activity in which a cyber thief impersonates the victim to fraudulently spend the victim's money.").

5. Opderbeck, *supra* note 3, at 939.

6. *See* Katie Bo Williams, *Officials Worried Hackers Will Change Your Data, Not Steal It*, HILL (Sept. 27, 2015), http://thehill.com/policy/cybersecurity/254977-officials-worried-hackers-will-change-your-data-not-steal-it [perma.cc/VHJ5-KWPW] (noting that "as security systems get better and hackers are forced to get more creative, manipulation is a likely new cyber vanguard"); Orestis Papakyriakopoulos et al., *Social Media and Microtargeting: Political Data Processing and the Consequences for Germany*, BIG DATA & SOC'Y 1, 2 (2018) (citation omitted) ("[M]icrotargeting presupposes the collection of large amounts of data able to depict the political preferences and other non-political characteristics of voters. . . . Another advantage is that microtargeting allows political actors to target voters from the entire political spectrum, rather than exclusively developing their campaign on the characteristics of the *median voter*, as was the case in the past.").

7. I have previously argued that current data-breach law should be read broadly and amended as needed. *See* Ido Kilovaty, *Data Breach Through Social Engineering*, HARV. L. REV. BLOG (Mar. 21, 2018), https://blog.harvardlawreview.org/data-breach-through-social-engineering [perma.cc/3LVP-XKTW] ("[W]e should be rethinking our conception of what

explores whether cybersecurity law, in particular data-breach notification law, is able to address these new threats to individual autonomy, privacy, and democracy.

This Article argues that the current threat of online manipulation, as well as other emerging threats online that transcend dated notions of identity theft and financial fraud, require a significant reevaluation, and as a result, an update of the scope and concept of cybersecurity law. This Article calls for an expansion of the meaning of cybersecurity law to include not only data breaches that present some actual risk of identity theft or fraud, but also data breaches that breach *autonomy* and *democracy*.[8] This Article defines cybersecurity law as the statutes that focus on data security, data-breach notification, post-breach litigation based on common law and statutory claims, computer hacking laws, and laws on information sharing.[9] Today's data breaches call for a reconceptualization of the law, informed by the concept of information fiduciaries, which among other things, requires that Internet actors secure user information.[10] While this law is largely a decentralized patchwork, the

constitutes a data breach, and subsequently, what sort of activities we wish to delegitimize through our legal system. The statutes can and should be read broadly to include socially engineered breaches; where the law is not sufficiently clear about this, it should be amended. Once we acknowledge that a data breach could take place in the form of manipulation, we could provide better protection for user privacy and security. This would in turn incentivize tech companies to monitor third-parties with whom they share user personal data, and make it harder for malicious actors to take hold of that data."); *see also* Patricia Hurtado, *Schneiderman Says New York Data Law 'Outdated and Toothless'*, BLOOMBERG (Mar. 29, 2018), https://www.bloomberg.com/news/articles/2018-03-29/schneiderman-says-new-york-data-law-outdated-and-toothless [perma.cc/KTU9-PKPD] (reporting that New York Attorney General Eric Schneiderman announced that he would introduce legislation that would require online service providers to notify "consumers when they learn that users' personal information was misused").

8. For an argument on how the current data economy enables democracy to be "hacked," see Hugo Zylberberg, *Democracy, Hacked: A Security Argument for Data Protection*, LAWFARE (Jan. 26, 2017), https://www.lawfareblog.com/democracy-hacked-security-argument-data-protection [perma.cc/82HG-RB3K] ("[T]he business model of the Newsfeed rests on the profit generated by this '*targeting-and-convincing' infrastructure*. First, companies like Facebook or Twitter collect personal data on their users to profile them (the targeting phase). Second, these segments of users are served ads that are paid for by third parties (the convincing phase). If the ad content shifts from commercial to political, Facebook and Twitter's Newsfeed algorithms can thereby be co-opted into a 'micro-propaganda machine.' This machine, during election cycles, can then be exploited not just by companies but also for the political purposes of either national or foreign organizations. Indeed, the massive collection of personal data has enabled political entrepreneurs, both at home and abroad, to hack democracy.").

9. Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 1011 (2018) (listing the statutes that would fall under the definition of U.S. data security statutes).

10. The concept of information fiduciaries could apply in cases of autonomy breaches. As Jack Balkin suggests in a blog post on the political economy of freedom of speech,

regulatory model behind it is primarily focused on financial harms.

A. CYBERSECURITY & DATA-BREACH NOTIFICATION LAW

Cybersecurity law itself is a fairly broad concept. It involves a patchwork of federal and state statutes and regulations—an "uncoordinated mishmash" of sorts.[11] Cybersecurity law is not fully capable of protecting the three basic aspects of information security: confidentiality, integrity, and availability.[12] Data-breach notification law, the focus of this Article, represents certain tradeoffs, balances, and priorities set by cybersecurity law. It reflects the goals that cybersecurity law sets for itself—primarily protection from and mitigation of identity theft and financial fraud. Data-breach notification law deals with a very concrete aspect of cybersecurity—post-breach notification. Though notification presupposes that a data breach has occurred and that the breached entity is under an obligation to notify its consumers, both requirements are the basic building blocks of data-breach notification law.[13] Data-breach notification laws represent the broader inability of cybersecurity law to adapt to new threats presented by the abuse of personal and nonpersonal information. The consideration of data-breach notification law as the first step in responding to manipulation may facilitate the development of other cybersecurity statutes. The inclusion of manipulation within the scope of incidents covered by data-breach notification law can further develop and

> if you want a simple example of what difference the concept of information fiduciaries would make, take a look at the recent Facebook/Cambridge Analytica scandal. It's important to focus not only on the particular example of Facebook's negligence in dealing with Alexsandr Kogan and Cambridge Analytica, but also on the ensuing revelations: Facebook's practices were merely the tip of a far larger iceberg—a series of unwise decisions through which Facebook allowed its business partners to access its end-users' social graphs. In my view, Facebook probably violated all three duties of care, confidentiality and loyalty. Facebook did not take sufficient care to vet its business partners, it breached its duties of confidentiality toward its end users, and it allowed its end-users to be manipulated by its business partners.

Jack M. Balkin, *The Political Economy of Freedom of Speech in the Second Gilded Age*, LAW & POL. ECON. (July 4, 2018), https://lpeblog.org/2018/07/04/the-political-economy-of-freedom-of-speech-in-the-second-gilded-age [perma.cc/8CHG-EMH6].

11. Kosseff, *supra* note 9, at 988.

12. *See* CHARLES P. PFLEEGER ET AL., SECURITY IN COMPUTING 7 (5th ed. 2015).

13. CAL. CIV. CODE § 1798.82 (West 2019) (requiring data breach notification invocation once a: (1) "breach of the security of the system" occurs and; (2) the breached entity determines that there aren't any factors precluding notice to consumers). These factors vary by state and may include an ongoing law enforcement investigation or a determination that there is no risk of harm to consumers.

inform other cybersecurity statutes on what ought to be protected.[14] This expansion is part of a larger trend associated with cybersecurity law—its two dominant regulatory models, information sharing and deterrence.[15]

While data-breach notification law has played an important, albeit imperfect,[16] role in addressing the more traditional form of data breaches, it has failed to address risks other than identity theft or financial fraud.[17] For example, there is a risk that breached information will be used for online manipulation and microtargeting as a direct result of a data breach. Although many concerns exist in today's data-breach landscape, this Article focuses on online manipulation through psychographic profiling to demonstrate the advanced threats presented by data breaches.[18] The failure to contain the effects of online manipulation is attributed not to the law or to its structure alone. Actually, the law on data breach notification has some plasticity that would allow it to apply to new cybersecurity threats in the same manner that it currently applies to identity theft and fraud. The problem, rather, is how the law is being perceived, applied, adjudicated, and used in different contexts. It is a question of the foundations of cybersecurity law, whether these foundations work today, and whether we should reevaluate what they ought to be.

B. BIG DATA & MANIPULATION

A lot can be said about how emerging technological advances bolstered the ability to analyze and use data in new and sophisticated ways.[19] While data

14. *See* Jeff Kosseff, *Cybersecurity of the Person*, 17 FIRST AMEND. L. REV. 343, 345 (2018) (arguing that cybersecurity law is narrowly focused on financial fraud and identity theft but should also apply to new harms that include "non-economic harms, such as online harassment, cyberbullying, and revenge pornography").

15. Andrea Matwyshyn, *Cyber!*, 2017 BYU L. REV. 1109, 1126–27 (2018).

16. Some scholars refer to this imperfection as "data breach fatigue." *See* Mathew Ingram, *Are We All Suffering From Data Breach Fatigue?*, COLUM. JOURNALISM REV. (Oct. 3, 2018), https://www.cjr.org/the_media_today/facebook-data-breach.php [perma.cc/HJ8N-WT7Y].

17. Kosseff, *supra* note 9, at 358 ("What do data breach notification laws not cover? For starters, they do not require individuals to be notified of the disclosure of information that could be used to stalk, harass, or dox them.").

18. *See, e.g.*, Daniel Castro, *It Would Have Taken More Than Privacy Laws to Prevent the Cambridge Analytica Scandal*, HILL (Apr. 10, 2018), http://thehill.com/opinion/technology/382443-it-would-have-taken-more-than-privacy-laws-to-prevent-the-cambridge [https://perma.cc/Z92Y-G6SL] (arguing that privacy laws have failed in protecting user data from Cambridge Analytica, thus claiming that the private sector should find solutions to the problem of online manipulation in the future, rather than legislators).

19. *See* Louise Amoore & Volha Piotukh, *Life Beyond Big Data: Governing with Little Analytics*, 44 ECON. & SOC'Y 341, 344 (2015) ("[O]ne of the many problems with a pervasive focus on 'big' and 'data' is that the finite and granular minutiae of the analytics are

has always had its face value—derived from its representation of certain information about something or someone—its value nowadays also originates from the ability to make sense of it on a higher level, a secondary use of sorts enabling software to explain patterns and inferences based on thousands of variables.[20] This secondary use provides a deeper insight into the data subject's personality, weaknesses, vulnerabilities, and more.

This "big data" is becoming increasingly valuable due to what machine learning algorithms can do with it. Primarily, big data may reveal patterns, abnormalities, and trends that are not visible to the naked human eye. Its capability and success rate in doing so are also gradually increasing based on user feedback and outcomes, making inferences informed by psychology, sociology, and behavioral economics.[21] On a more individual level, highly detailed and nuanced data about someone, paired with advanced technology and insights from online behaviorism, allows for malicious actors to more effectively manipulate the individual by exploiting existing biases and vulnerabilities.[22] While manipulation has existed throughout human history as part of human interaction,[23] today, manipulation proliferates on the Internet,

overlooked."). However, certain commentators cast doubt on the assertion that big data has some exceptional power or utility for the purpose of prediction of behaviorism. *See, e.g.*, Caryn Devins et al., *The Law and Big Data*, 27 CORNELL J.L. & PUB. POL'Y 357, 371–72 (2017) ("Big Data's supposed objectivity and predictive power are overstated, at least when applied to highly complex evolutionary systems such as the legal system. Data always require interpretation, which necessitates theory and, correspondingly, evaluative judgment by humans. Further, Big Data cannot foresee the fundamentally creative, non-algorithmic evolution of the legal system, and its predictive power is limited.").

20. *See* Sofia Grafanaki, *Autonomy Challenges in the Age of Big Data*, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 803, 805 (2017) (describing the future of algorithmic regulation, "where decisions about individuals and society in general are made by software taking into account thousands of variables not interpretable in human language").

21. *See* Karen Yeung, *'Hypernudge': Big Data as a Mode of Regulation by Design*, 20 INFO., COMM. & SOC'Y 118, 119 (2017) ("[T]he technology and the process comprise a methodological technique that utilises analytical software to identify patterns and correlations through the use of machine learning algorithms applied to (often unstructured) data items contained in multiple data sets, converting these data flows into a particular, highly data-intensive form of knowledge.").

22. *See* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 999 (2014) (identifying the role of behavioral economics in manipulating consumers: "[t]he interplay between rational choice and consumer bias that is at the heart of behavioral economics helps illustrate how information and design advantages might translate into systematic consumer vulnerability").

23. *See* Marcello Ienca & Effy Vayena, *Cambridge Analytica and Online Manipulation*, SCI. AM. (Mar. 30, 2018), https://blogs.scientificamerican.com/observations/cambridge-analytica-and-online-manipulation [perma.cc/7JBG-MTFK] ("Attempts to manipulate other people's unconscious mind and associated behavior are as old as human history. In Ancient Greece, Plato warned against demagogues: political leaders who build consensus by appealing

media, politics, markets, family, friendships, relationships, and life.[24]

But recent technological advancements, the availability of data, and the global nature of the Internet give manipulation a far more menacing form, especially as manipulation becomes pervasive in U.S. political processes and culture.[25] As some commentators put it—"[s]ince we are never totally free of outside influence, what gives us (part) authorship over our own actions is that we regard our own reasons for acting as authoritative. Manipulation thwarts that."[26]

C. INFORMATION FIDUCIARIES

The enormous scope of adverse effects and emerging information practices brought about by new technologies requires government regulation that would mitigate the harms anticipated from their use or requires that the industry self-regulate by enacting precautionary measures to decrease the likelihood that such harms would materialize.[27]

For example, Jack Balkin's *Information Fiduciaries in the Digital Age* argues that we create a fiduciary obligation upon Internet platforms when we entrust them with our information assets in order to keep our information confidential and secure.[28] Online service providers would assume these duties because they

---

to popular desires and prejudices instead of rational deliberation. However, the only tool demagogues ancient Athens could use to bypass rational deliberation was the art of persuasion. In today's digital ecosystem, wannabe demagogues can use big data analytics to uncover cognitive vulnerabilities from large user datasets and effectively exploit them in a manner that bypasses individual rational control.").

24. *See* Cass R. Sunstein, *Fifty Shades of Manipulation*, 1 J. MARKETING BEHAV. 213, 218 (2015).

25. Roberto J. González, *Hacking the Citizenry? Personality Profiling, 'Big Data' and the Election of Donald Trump*, 33 ANTHROPOLOGY TODAY 9, 11 (2017) (explaining how personality profiling software and tools have been used since Obama's 2012 presidential campaign).

26. Helen Nissenbaum et al., *Online Manipulation: Hidden Influences in a Digital World* 16 (Jan. 8, 2019) (unpublished manuscript) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3306006 [https://perma.cc/4KJU-DABA].

27. *See, e.g.*, *What is App Review For Facebook Login*, FACEBOOK https://developers.facebook.com/docs/facebook-login/review/what-is-login-review [perma.cc/UG8H-T87J] (last visited Aug. 13, 2019) (describing a process developed by Facebook following the Cambridge Analytica scandal to ensure that developers are transparent and accountable to their uses of Facebook user data). For a critical view of self-regulation in the manipulation context, see Terrell McSweeny, *Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is The FTC Keeping Pace?*, 2 GEO. L. TECH. REV. 514, 514 (2018), in which McSweeny notes that the phenomena of online manipulation and influence "underscore the power of increasingly sophisticated predictive technology and the limitations of the United States' largely self-regulatory approach to consumer data rights, privacy, and security."

28. *See generally* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016).

act as information fiduciaries.[29] As information fiduciaries, a person or business dealing with sensitive information should "have duties of care, confidentiality, and loyalty toward the people whose data they collect, store, and use."[30]

While the importance of the imposition of these duties cannot be overstated, serious limitations exist to imposing such duties directly on online service providers when it comes to online manipulation. The fiduciary approach assumes business-as-usual and does not consider the proliferation of data breaches that compromise the same information held by these information fiduciaries. These data breaches may trigger information fiduciaries' duty of loyalty to their customers.[31] Failing to protect that information, and perhaps even the collection of certain information, may breach that duty. Similarly, failing to notify regulators or consumers that a breach has occurred ought to violate that duty. In the context of data breach, the duty of loyalty would require additional steps that would guide companies on how to notify their consumers and approach the issue. While holding online service providers as information fiduciaries may mitigate some of the risks associated with data compromise, it does not fully capture data that does not seem "sensitive" or relationships between customers and entities that are not deemed fiduciaries.

Expanding data-breach notification law is not only a response to the information fiduciaries approach, but also a legal intervention (in particular, through tort law) to the mere enablement of online manipulation by these fiduciaries.[32] After all, the failure to secure personal information may create

29. *See* Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/ [perma.cc/Y46P-PPJW] ("An *information fiduciary* is a person or business that deals not in money but in information. Doctors, lawyers, and accountants are examples; they have to keep our secrets and they can't use the information they collect about us against our interests. Because doctors, lawyers, and accountants know so much about us, and because we have to depend on them, the law requires them to act in good faith—on pain of loss of their license to practice, and a lawsuit by their clients. The law even protects them to various degrees from being compelled to release the private information they have learned.").

30. Balkin, *supra* note 10.

31. In general, an information fiduciary is an extension of the general fiduciary duty in law. *See* Balkin & Zittrain, *supra* note 29 ("In the law, a *fiduciary* is a person or business with an obligation to act in a trustworthy manner in the interest of another. Examples are professionals and managers who handle our money or our estates. An information fiduciary is a person or business that deals not in money but in information.").

32. Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1558 (2005) (exploring the idea that certain software vulnerabilities and defects enable cybercrime and therefore should be considered a tort: "[t]he software industry has simply abdicated to third parties its responsibility for limiting high-risk

new threats against the data subjects who lose their information. As online service providers collect ever-increasing amounts and categories of data about us, regardless of whether this data was given voluntarily or involuntarily,[33] malicious actors are increasingly empowered by the availability of such data troves for the purpose of manipulation.[34] Intervening through data-breach notification law could therefore resolve some of the difficulties with third-party misuse of personal information, since these parties are rarely in direct contractual relationships with the manipulated victims.[35] This would effectively shift the disclosure and mitigation burden back to the breached entity.

Current data-breach notification law could potentially mitigate online manipulation, but current data-breach jurisprudence emphasizes a strict tangibility approach. Under this framework, the legitimacy of a claim for harm caused by a data breach hinges upon the actual, *tangible* harm sustained by the victims, not whether an *intangible* harm took place or risk of such harm increased.[36]

---

design defects. 'The problem is that those responsible for securing our personal data are rarely the ones who pay the cost of securing it and in many cases are not the same people with whom we have entrusted our data in the first place' ") (citation omitted).

33. *See* Daniel Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1411 (2001). It is understood that online service providers obtain personal data about us in two ways—"(1) by directly collecting information from users (registration and transactional data); and (2) by surreptitiously tracking the way people navigate through the Internet (clickstream data)." *Id.*

34. *See* Alexis Madrigal, *What Took Facebook So Long?*, ATLANTIC (Mar. 18, 2018), https://www.theatlantic.com/technology/archive/2018/03/facebook-cambridge-analytica/555866 [perma.cc/KQ8H-RE4P] ("If one were to systematically crawl through all the data that could be gleaned from just a user's basic information, one could build a decent picture of that person's social world, including a substantial amount of information about their friends.").

35. *See* McSweeny, *supra* note 27, at 517–18 ("However, this framework [FTC enforcement] does not address the use of personal information by third parties and data brokers who have no direct consumer-facing relationship, nor does it adequately reach unanticipated uses of data as inputs for complex algorithms or by the increasingly powerful platforms that mediate most consumers' Internet experience.").

36. *See, e.g.*, Bradix v. Advance Stores Co., No. 16-4902, 2016 WL 3617717, at *1–4 (E.D. La. July 6, 2016) (dismissing a claim of injury because the misuse by criminals of breached personal information for car financing did not affect the plaintiff's credit score); *In re* SuperValu, Inc., Customer Data Sec. Breach Litig., No. 14-MD-2586, 2016 WL 81792, at *8 (D. Minn. Jan. 7, 2016) (dismissing the lawsuit because a single plaintiff's unauthorized credit card charge does not constitute harm and therefore the plaintiff lacks standing); Doe v. Chao, 540 U.S. 614, 625 (2004) (the government sending social security numbers to unauthorized parties [therefore violating the Privacy Act of 1974] does not constitute harm); *see also* Daniel Solove & Danielle Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 755 (2018) (discussing the absurdity of not recognizing other data-breach harms, such as anxiety and risk: "[r]equiring harm to be visceral and vested has severely restricted the recognition of data-breach harms, which rarely have these qualities. Data-breach harms are not easy to see, at least not in any physical way. They are not tangible like broken limbs and

This outdated approach fails to recognize a neoteric, and perhaps more devastating type of personal information misuse—manipulation—a harm that is different from identity theft or fraud and which transcends the notion of pure economic injury.[37] The current focus of data-breach jurisprudence is therefore ineffective and increasingly irrelevant in today's data analytics reality, requiring a conceptual adaptation and transformation.

What is currently missing from the literature is a comprehensive account of the evolving and necessary role of data-breach notification law and how it could be leveraged to meet the future landscape of data exploitation before regulators create more advanced and direct forms of norms and regulations. This Article addresses this gap.

This Article contributes to the literature by advancing two main arguments. First, the risk of online manipulation resulting from a data breach should be sufficient grounds to trigger data-breach notification law. In other words, the question is whether there was a loss of information that can objectively be used for microtargeting, or any other harm that would not qualify as either identity theft or financial fraud. This would mean that breached companies would have to inform consumers and regulators when there is a risk of manipulation associated with compromised personal information, even if there is no risk of identity theft or fraud. Second, adopting such legal intervention would result in crucial benefits for society and the digital ecosystem—reducing the information asymmetry between consumers and firms, indirectly regulating data collection, increasing information security, remedying manipulation of victims, and strengthening regulatory oversight over data collectors.[38] While we may believe that new socio-technological problems require tailored regulatory solutions, and indeed many of them do in the long-term, this is not necessarily the case in the interim, where existing tools may still prove useful

destroyed property. Instead, the harm is intangible. Data breaches increase a person's risk of identity theft or fraud and cause emotional distress as a result of that risk. Despite the intangible nature of these injuries, data breaches inflict real compensable injuries. Data breaches raise significant public concern and generate legislative activity"); Ashenmacher, *supra* note 4, at 5 ("But have individuals been harmed even where their PII [personally identifiable information] has not been used to commit fraud? . . . By and large, American law has responded with an unsympathetic 'no.' "); Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2279 (2015) ("If people's data are leaked, but they do not suffer from identity theft, are they harmed? Although courts struggle to recognize harm, there clearly seems to be a substantial negative impact on people's lives.").

37. *See* Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 70 (2003) ("[T]he appropriation tort . . . is aimed at protecting a broader sphere of identity than mere names or physical likenesses and . . . [it] is intended to protect dignitary, rather than economic, interests.").

38. *See infra* Part IV.

in addressing these challenges.

The Article proceeds as follows. Part I explores the tenets of online manipulation in the context of psychographic profiling and provides an analysis of the perils of manipulation and how manipulation threatens autonomy, democracy, and freedom from experimentation. Part II provides an overview of where current data-breach notification law stands when it comes to data being misused for targeted user manipulation, highlighting some of the gaps that require reevaluation in light of online manipulation practices. Part III explores the ways in which embedding online manipulation within data-breach notification law would benefit society and consumers at large. It considers and builds on existing scholarship on privacy harms, cybersecurity and data-breach litigation, and online manipulation.[39] In addition, this Part will also address some of the hurdles requiring further research on how to meet these challenges. Finally, the Article concludes in Part IV by proposing a reconceptualization of data-breach jurisprudence to meet a world of digital manipulation.

II. ONLINE MANIPULATION AND PSYCHOGRAPHIC PROFILING

Manipulation for marketing and other purposes is not a novel phenomenon. In the late 1950s, motivational analysis gave rise to "depth marketing,"[40] which allowed advertisers to target potential consumers through subliminal advertising, increasing the likelihood that consumers would purchase a product.[41] Scholars first raised concerns over privacy stemming from manipulation in 1971,[42] and today it draws even more attention from legal academics.[43]

39. *See, e.g.*, Solove & Citron, *supra* note 36, at 737; Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011); Ryan Calo, *Privacy Harm Exceptionalism*, 12 COLO. TECH. L.J. 361 (2014); Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125 (2015); Sunstein, *supra* note 24; Tansy Woan, *Searching for an Answer: Can Google Legally Manipulate Search Engine Results?*, 16 U. PENN. J. BUS. L. 294 (2013); Susser et al., *supra* note 23.

40. *See generally* VANCE PACKARD, THE HIDDEN PERSUADERS (1957).

41. Calo, *supra* note 22, at 997.

42. *See* ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 442–43 (1971) (predicting risks that threaten the "line between the use of cybernetics to understand an individual and its use to control or affect his conduct . . . [which] is shadowy at best").

43. Sunstein, *supra* note 24; *see generally* Eric Posner, *The Law, Economics, and Psychology of Manipulation*, (Coase-Sandor Inst. for Law and Econ., Working Paper No. 726, 2015).

In *Digital Market Manipulation*, Ryan Calo explores the question of manipulation for marketing purposes. Focusing on the new legal and ethical questions that such a phenomenon raises, Calo asks whether at a certain point, these techniques reach a level of severity and misalignment of interests between the manipulator and manipulee that justifies legal intervention.[44] Calo mentions information-based interventions focused on mandatory disclosure as an example of a legal intervention seeking to minimize, or even negate, the harm of manipulation.[45] If manipulation subjects are informed, the potency of manipulation may be weakened, though it may not fully disappear.[46] The same information-based intervention needs to be explored with regard to online manipulation, not solely for marketing, but even more so for political and ideological purposes, e.g., microtargeted political ads that leverage individual vulnerabilities and personality traits.[47] If a sufficiently sophisticated and motivated entity obtains access to a diverse set of data points about each individual, it would be able to construct manipulatable personality profiles and exploit them. Indeed, Calo considers "how should law or society treat political ads by candidates or causes that leverage individual biases to make their campaigns more effective? Such techniques portend an arguably greater threat to autonomy."[48] Calo does not directly answer this question.

Different U.S. presidential campaigns have similarly used "symbolic manipulation by design, playing on deeply held beliefs in the electorate" to improve their chances of success in the election.[49] Technology makes these efforts much easier, more effective, and potentially more dangerous for protected values like free speech, autonomy, and democracy.[50] Because

44. Calo, *supra* note 22, at 998.

45. *Id.* at 1013.

46. This intuition dates back to 1914, when Louis Brandeis claimed that "[p]ublicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants . . . ." LOUIS BRANDEIS, *What Publicity Can Do*, *in* OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT 92, 92 (1914).

47. *See* Frederik J. Zuiderveen Borgesius et al., *Online Political Microtargeting: Promises and Threats for Democracy*, 14 UTRECHT L. REV. 82, 82 (2018) ("Through political microtargeting, a political party can identify the individual voters which it is most likely to convince. Additionally, a party can match its message to the specific interests and vulnerabilities of these voters. Modern online marketing techniques promise to make microtargeting even more tailored to individual voters, and more effective.").

48. Calo, *supra* note 22, at 1049.

49. J.R. McLeod, *The Sociodrama of Presidential Politics: Rhetoric, Ritual, and Power in The Era Of Teledemocracy*, 101 AM. ANTHROPOLOGIST 359, 360 (1999).

50. *See* Zeynep Tufekci, *Facebook and Engineering the Public*, MEDIUM (June 29, 2014), https://medium.com/message/engineering-the-public-289c91390225 [perma.cc/TV56-NYLM] ("[T]hese large corporations (and governments and political campaigns) now have new tools and *stealth* methods to quietly model our personality, our vulnerabilities, identify our networks, and effectively nudge and shape our ideas, desires and dreams. These tools are new,

politicians can continue to capitalize on the perceived political advantages without being held accountable for the many dangers, these manipulation efforts will likely persist in the political context.[51] This is not the sole reason why legal intervention is now needed, but it exacerbates the privacy and autonomy challenges arising from online manipulation.

Online manipulation may sound like an overly broad concept, with some parts of it justifying legal intervention while others do not.[52] It could vary in degree, intrusiveness, sophistication, motives, purpose, actors, and tools.[53] As Daniel Susser, Beate Roessler, and Helen Nissenbaum point out in their work *Online Manipulation*,[54] manipulation could take the form of a nudge, persuasion, deception, coercion, and more.[55] As Cass Sunstein puts it in *Fifty Shades of Manipulation*—"it has at least 50 shades."[56] Some of these shades are socially and legally acceptable, while others are not.[57] For example, persuasion is seen as a normal rhetorical tool, where "people are given facts and reasons, presented in a sufficiently fair and neutral way."[58] However, this would not be the case for severe coercion, where facts and reasons are not presented to people, but rather these people are forced into a choice they would otherwise not make.[59]

Given this divergent normativity, legal intervention will only be justified for some forms of manipulation and not for others. However, even when justified, it could be shaped in different ways—through direct regulation of the relevant industry (social media, political entities, data brokers, etc.), the data-subjects, or the incentives and disincentives that usually surround this

---

this power is new and evolving.").

51. *See* Nina Burleigh, *How Big Data Mines Personal Info to Craft Fake News and Manipulate Voters*, NEWSWEEK (June 8, 2017), http://www.newsweek.com/2017/06/16/big-data-mines-personal-info-manipulate-voters-623131.html [perma.cc/YRF5-D7J2] ("By 2020, behavioral science, advanced algorithms and AI applied to ever more individualized data will enable politicians to sell themselves with ever more subtle and precise pitches.").

52. *See* Nissenbaum et al., *supra* note 26.

53. *Id.*

54. *Id.*

55. *Id.*

56. Sunstein, *supra* note 24, at 216.

57. *See* Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1150 (2011) (arguing, for example, that coercion exists on a spectrum, which determines its permissibility: "[m]any important activities, from air travel to medical care, are premised upon giving up information or revealing one's body in potentially demeaning and uncomfortable ways. There may indeed be little alternative to surveillance in daily life").

58. Sunstein, *supra* note 24, at 216.

59. *See id.* at 220; *see also* JOSEPH RAZ, THE MORALITY OF FREEDOM 377 (1988) (contrasting coercion from manipulation by providing that "[m]anipulation, unlike coercion, does not interfere with a person's options. Instead it perverts the way that person reaches decisions, forms preferences or adopts goals").

manipulation phenomenon. Manipulations should warrant certain legal intervention in such cases where personal and nonpersonal information can be used in ways that are likely to affect a person's thoughts, opinions, and actions. This Article will use the definition of manipulation developed by Nissenbaum et al.—"imposing a hidden influence on someone by targeting and exploiting their weaknesses or vulnerabilities."[60]

There are three fundamental components in this definition. First, the manipulation is hidden from the subject, known to the manipulator, and known or unknown to different degrees to others.[61] Data-breach notification law seeks to address exactly this information gap by exposing the existence of a breach and ensuring that potential victims take extra precautions.[62] Second, the manipulation exploits weaknesses and vulnerabilities of the subject based on data available about her. Manipulators learn these weaknesses and vulnerabilities by using advanced algorithms to analyze thousands of different data points and create a certain personality profile.[63] And, third, the manipulation must be targeted, meaning that the subject gets served with a certain communication tailored precisely to gain access to the attention, interest, and hopefully action of that individual, whether cognitive or behavioral. While manipulation can be achieved through a variety of techniques, manipulation becomes particularly alarming with the emerging technique of psychographic profiling.[64]

60. Nissenbaum et al., *supra* note 26, at 22.

61. *See* Nissenbaum et al., *supra* note 26, at 16 ("The hiddenness of manipulative influences explains how it is possible to alienate someone from their own decision-making powers.").

62. *See* Sasha Romanosky et al., *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 J. POL'Y ANALYSIS & MGMT. 256, 262 (2011) ("Consumer precaution should increase after the passage of the law because, as more consumers are notified of a breach involving their sensitive information, they may take steps to reduce the risk and the costs of becoming a victim of identity theft. For example, they could notify their financial institutions to block transactions and cancel accounts or apply credit freezes and fraud alerts. Moreover, such notices also could serve to increase consumer awareness in general, making them alert to possible identity thefts. Therefore, a primary effect of data breach disclosure laws should be the reduction of the incident of identity theft, as well as a mitigation of its impact, via better consumer precaution.").

63. *See* Katy Steinmetz, *The Facebook Data Cambridge Analytica Took Was Either Extremely Valuable or Totally Worthless*, TIME (Mar. 22, 2018), http://time.com/5207764/cambridge-analytica-facebook-data [perma.cc/T42W-M7LB] ("The trove included information like people's names, locations, genders and things users have "liked" on Facebook, which a company whistleblower said it planned to use to exploit "the mental vulnerabilities of people" with targeted political messages . . . the firm's [Cambridge Analytica] intention [was] to use "likes" to help build algorithms that can predict the personality traits of voters.").

64. *See infra* Section II.A.

To be clear, data-breach notification law is but one solution to a broader cybersecurity law problem, and online manipulation is an emerging threat that cybersecurity law should be concerned with, but it is one harm out of many. Jeff Kosseff, for example, argues that cybersecurity law is overly reliant on financial harm, whereas there is a myriad of other online harms that cybersecurity law should adapt to, such as risk, anxiety,[65] revenge pornography, and online harassment.[66] Psychographic profiling is a case study which highlights the emerging cybersecurity harms that law should respond to.

A. PSYCHOGRAPHIC PROFILING AS MANIPULATION

Psychographic profiling (or psychographics) is a technique that creates a personality profile of an individual based on five main personality traits. Social psychologists have long recognized the ability to profile individuals based on the "Big Five" personality traits: openness, conscientiousness, extroversion, agreeableness, and neuroticism.[67] Initially, psychographic profiling was ineffective due to data collection problems. However, data collection problems have been resolved due to the wide availability of data.[68] Psychographic profiling does not necessarily have to be nefarious. For example, it could be used to motivate people to engage in healthier activities and habits,[69] as well as make consumers more comfortable and their experiences more convenient. However, to date, these targeting methods hold the most potential when it comes to influencing and manipulating individuals.[70]

In 1999, entrepreneur Thomas Gerace created a patent that provided an early example of how computer systems could incorporate psychographic profiling. Gerace created a computer program that determined the

65. *See generally* Solove & Citron, *supra* note 36.

66. *See generally* Kosseff, *supra* note 11, at 355.

67. González, *supra* note 25, at 10.

68. *See generally* Ali Fenwick, *Psychographics: How Big Data is Watching You*, HULT BLOG (2018), https://www.hult.edu/blog/psychographics-big-data-watching/ [https://perma.cc/9TEM-TSC7].

69. *See generally* Sarah Hardcastle & Martin Hagger, *Psychographic Profiling for Effective Health Behavior Change Interventions*, 6 FRONTIERS PSYCHOL., Jan. 2016, at 1, 1–2 ("Research has identified multiple correlates of health behavior change, and interventions have been developed to target these factors. Such interventions have shown significant effects in changing behavior" though, researchers believe that a more individualized form of intervention may be required to be more effective overall.").

70. *See generally id.*; Kalev Leetaru, *Data Breaches, Psychological Profiling, Voter Modeling: Inside the Big Data World of Campaign 2016*, FORBES (Jan. 1, 2016), https://www.forbes.com/sites/kalevleetaru/2016/01/01/data-breaches-psychological-profiling-voter-modeling-inside-the-big-data-world-of-campaign-2016/#4ffc8def7c4f [perma.cc/6CMY-EBHH] ("This is the future of political campaigning in the 21st century in which we are all just data points in giant psychographic models that attempt to figure out how best to make us vote a certain way.").

psychographic profile of a user based on her "history and/or pattern of user activity which in turn [was] interpreted as a user's habits and/or preferences."[71] This sort of dataset is explicitly distinguished from demographics, where only personal details such as gender, age, income bracket, and occupation are taken into account.[72] This distinction, even tension, between demographics and psychographics is crucial to realizing that a reform of data-breach notification law is desperately needed, since data-breach law is for the most part concerned with demographic information. This will be discussed further in Part IV of this Article.

Manipulation by itself is not an absolute evil. Rather, it depends on whether there is an alignment of interests between the subject and the manipulator, both on the individual and collective levels.[73] As Calo aptly suggests, legal intervention would be justified whenever there is a divergence between these interests, leading to one side leveraging this gap in information to her own benefit.[74] This is where the regulator should intervene.

Recently, the British political consultancy firm, Cambridge Analytica, used psychographic profiling to conduct political manipulation, allegedly influencing the outcomes of the 2016 U.K. referendum to withdraw from the European Union,[75] and the 2016 U.S. presidential election.[76]

Cambridge Analytica, a counterpart of the data mining and analysis firm SCL Group, has become infamous for improperly accessing the sensitive and personal information of 87 million Facebook users in an unauthorized manner.[77] This personal information was obtained through data collected by a "test your personality" research application (app) developed by a University of Cambridge neuroscience lecturer, Aleksandr Kogan, using the Facebook application programming interface (API).[78] The data collected by this app was

71. U.S. Patent No. 5,991,735 (issued Nov. 23, 1999).

72. *Id.*

73. *See* Calo, *supra* note 22, at 1023.

74. *Id.*

75. *See generally* Carole Cadwalladr, *The Great British Brexit Robbery: How Our Democracy Was Hijacked*, GUARDIAN (May 7, 2017), https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy [perma.cc/24RV-LT2R] ("Cambridge Analytica . . . the data analytics firm that played a role in both Trump and Brexit campaigns.").

76. González, *supra* note 25, at 9.

77. *See* Issie Lapowsky, *Facebook Exposed 87 Million Users to Cambridge Analytica*, WIRED (Apr. 4, 2018), https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica [perma.cc/HJL8-BNRN].

78. Ethan Zuckerman, *This Is So Much Bigger Than Facebook*, ATLANTIC (Mar. 23, 2018), https://www.theatlantic.com/technology/archive/2018/03/data-misuse-bigger-than-facebook/556310 [perma.cc/EL2X-7CGA] ("Aleksandr Kogan, the Cambridge University researcher who built a quiz to collect data on tens of millions of people, didn't break into

then passed on to Cambridge Analytica, in what some would assert to be a clear breach of research ethics.[79]

Cambridge Analytica, hired by the Leave.EU campaign[80] as well as Donald Trump's[81] and Ted Cruz's[82] presidential campaigns, offered these campaigns the data obtained from the app, and more importantly—the analytics based on that data. For example, when working for the Cruz campaign, Alexander Nix, then CEO of Cambridge Analytica, explained that the consultancy firm focused on 45,000 likely Iowa Republicans participating in the caucus who needed a little "persuasion message" to vote for Cruz.[83] Cambridge Analytica's psychographic profiling technique managed to craft targeted messages to voters based on "close to 4- or 5,000 data points on every adult in the United States."[84] Cambridge Analytica's use of data for effective manipulation through psychographic profiling reflects the striking breadth of data points and their analytical potential, which are part of a "data rich society, in which specific entities have the ability to collect and utilize an immense amount of data about a single individual."[85] This technique of manipulation has rightfully earned these techniques labels such as "mind-reading software" and "weaponized AI propaganda machine," which swayed voting preferences in many of its "persuadable" targets.[86] These methods were largely reconstructed based on tools developed by psychologist Michal Kosinski, who argued that digital records of an individual can reveal his or her personality traits to a high degree.[87]

Facebook's servers and steal data. He used the Facebook Graph API, which until April 2015 allowed people to build apps that harvested data both from people who chose to use the app, and from their Facebook friends.").

79. *See id.*

80. Carole Cadwalladr & Mark Townsend, *Revealed: The Ties That Bound Vote Leave's Data Firm to Controversial Cambridge Analytica*, GUARDIAN (Mar. 24, 2018), https://www.theguardian.com/uk-news/2018/mar/24/aggregateiq-data-firm-link-raises-leave-group-questions [perma.cc/A9VM-PJ42].

81. Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html [perma.cc/LEL3-P3P5].

82. Harry Davies, *Ted Cruz Using Firm That Harvested Data on Millions of Unwitting Facebook Users*, GUARDIAN (Dec. 11, 2015), https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data [perma.cc/6TEL-S3GY].

83. Nina Burleigh, *How Big Data Mines Personal Info to Craft Fake News and Manipulate Voters*, NEWSWEEK (June 8, 2017), http://www.newsweek.com/2017/06/16/big-data-mines-personal-info-manipulate-voters-623131.html [perma.cc/98JL-PKRB].

84. *Id.*

85. Tal Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRIES IN LAW 157, 169 (2019).

86. González, *supra* note 25, at 9.

87. *Id.* at 10.

Kosinski created a search engine for specific profiles—"all anxious fathers . . . all angry introverts . . . all undecided Democrats."[88] This enabled Cambridge Analytica to classify individuals within thirty-two distinct personality types—as well as slice and dice even further within these personality types—for the purpose of political microtargeting.[89] While some commentators are skeptical as to whether Cambridge Analytica was even remotely successful in its goal,[90] it is likely that the data harvested by Cambridge Analytica was used as a "training set" for future manipulation operations, which could prove successful.[91] A potential failure of today's manipulation efforts does not necessarily negate the threat indefinitely.

The intuition amongst many who have learned about Cambridge Analytica's dealings is that such manipulation is wrongful, as it unduly infringes on autonomy, democracy, and freedom from experimentation. But should manipulation be *legally* wrongful?[92] It is critical to understand what makes this phenomenon so wrongful that legal intervention is required.

B. THE WRONGFULNESS OF ONLINE MANIPULATION

What makes online manipulation so exceptional that it requires legal intervention? This Article makes three main arguments to support the claim that manipulation is wrong and therefore requires legal intervention. Although these arguments are most often discussed in the context of advertising and marketing, they are nonetheless applicable to the political context as well.

88. *Id.* (citing Hannes Grassegger & Mikael Krogerus, *The Data That Turned The World Upside Down*, MOTHERBOARD (Jan. 28, 2017), https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win [perma.cc/R9QL-PQ2U]).

89. JEFFREY C. SHUMAN ET AL., COLLABORATIVE COMMUNITIES: PARTNERING FOR PROFIT IN THE NETWORKED ECONOMY 68 (2001) (discussing potential developments in profiling tools that "slice and dice the reams of clickstream data Web sites collect into even finer descriptions of consumer profiles").

90. *See generally* Antonio Garcia Martinez, *The Noisy Fallacies of Psychographic Targeting*, WIRED (Mar. 19, 2018), https://www.wired.com/story/the-noisy-fallacies-of-psychographic-targeting [https://perma.cc/B23D-HGZ4] ("[I]f this psychographics business is so effective, why isn't it commonly used by smart e-commerce players like Amazon, or anyone else beyond the brand advertisers who like keeping old marketing folklore alive?").

91. *See* Alexis Madrigal, *What Took Facebook So Long?*, ATLANTIC (Mar. 18, 2018), https://www.theatlantic.com/technology/archive/2018/03/facebook-cambridge-analytica/555866 [https://perma.cc/4JWE-K6Z9].

92. *See generally* Andrew Keane Woods, *The Cambridge Analytica-Facebook Debacle: A Legal Primer*, LAWFARE (Mar. 20, 2018), https://www.lawfareblog.com/cambridge-analytica-facebook-debacle-legal-primer [perma.cc/QH95-7KMF] (discussing legal issues arising from Cambridge Analytica).

These arguments focus on autonomy,[93] democracy,[94] and experimentation.[95]

1. Autonomy

Online manipulation, if executed properly and successfully, is wrongful because it impairs the ability of individuals to make independent and informed opinions and decisions.[96] Manipulation infringes on individual autonomy because personal information is exposed to unauthorized entities and used to target the freedom of choice. It effectively deprives individuals of their agency[97] by distorting and perverting the way in which individuals typically make decisions.[98] This should be contrasted with rational persuasion, which is contrary to what manipulation stands for.[99]

Julie Cohen acknowledges that meaningful autonomy can be achieved through the adoption of robust information privacy laws and the protection of information relating to individuals and their personalities.[100] In her dynamic theory of information privacy, Cohen explains that in a no-privacy reality, surveilling individuals "will constrain, ex ante, the acceptable spectrum of belief and behavior."[101] However, manipulation affects far more directly the acceptable spectrum of belief and behavior. Therefore, manipulation violates autonomy not only through mere surveillance, but also through acting upon the data surveilled and against the data subject. While Cohen's work is concerned primarily with privacy, her conclusions on autonomy are equally applicable to emerging cybersecurity threats stemming from manipulation. Privacy and security are typically distinct when it comes to legal regulation, but

93. *See* Ashenmacher, *supra* note 4, at 8–31 (analyzing autonomy in the context of data-breach harms).

94. The literature originally focused on market manipulation, though in the political context, I would argue that it becomes a democracy concern, since democracy is the "market" equivalent in this context. *See, e.g.*, Jon D. Hanson & Douglas A. Kysar, *Taking Behavioralism Seriously: The Problem of Market Manipulation*, 74 N.Y.U. L. REV. 630 (1999).

95. *See* Zarsky, *supra* note 83, at 175 ("Yet a third way to articulate the manipulation-based argument is to note that such actions are unacceptable as they amount to human experimentation.").

96. Grafanaki, *supra* note 20, at 825 (explaining how predictive algorithms learn from past behavior of the subject, influencing his or her decisions in the future).

97. Sunstein, *supra* note 24, at 226.

98. Charles Mendez, *Deflating Autonomy*, 66 S.C. L. REV. 401, 413 (2014).

99. *The Ethics of Manipulation*, STAN. ENCYCLOPEDIA PHIL. (Mar. 30, 2018), https://plato.stanford.edu/entries/ethics-manipulation [perma.cc/3U67-WK8M] ("[I]t seems reasonable to think that because manipulation differs from rational persuasion, it must influence behavior by means that do not engage the target's rational capacities.").

100. *See* Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423 (2000).

101. *Id.* at 1426.

the manipulation threat concerns both privacy and security.[102]

Online manipulation not only constrains beliefs and behaviors ex ante, but it creates behavior in the manipulated subjects that would not necessarily take place had they not been manipulated, effectively depriving them of free and unimpaired choices. An act manipulates people if "it does not sufficiently engage or appeal to their capacity for reflection and deliberation."[103] A deontological objection suggests that manipulation negatively affects the ability "to assess, to weigh, to judge" at the actor's convenience and terms, without consenting to such influence.[104] However, this claim rests on the wrongfulness of the act of manipulation, rather than considering whether the manipulation was successful.

While autonomy is an individual-level concern, manipulation could also be wrongful because of its collective impact on democracy. Assuming an individual is successfully manipulated, the individual-level harm is negligible in the political sphere—say, one vote in favor of candidate A, instead of candidate B, out of millions of other voters. However, collectively, if a sufficiently large group of individuals is targeted by online manipulation, the results can be significant.[105] In that case, candidate A would gain a substantial advantage over candidate B, potentially impacting the electoral results.

Political processes throughout the world can be manipulated through social media in way that impairs voter's ability to autonomously reflect and rationalize individual choices. For example, the Russian interference in the 2016 U.S. presidential election and the U.K. referendum on the secession from the European Union (Brexit)[106] through social media herald the future of

102. *See* Matwyshyn, *supra* note 15, at 1140–41 ("Security refers to the hybrid scientific and legal inquiry into (1) whether particular implemented systems, products, and processes can successfully defend against all possible third-party attackers in both physical and digital space, and (2) what legal consequences arise when they cannot . . . . Privacy refers to the legal and policy inquiry regarding conflicts between (1) what information a person reasonably expects will be or can be collected and used about her (based in part on the legally-binding promises made to her, whose enforceability arises from dictates of either criminal or civil law), on the one hand, and (2) the technical and business reality of possible or actual collection and repurposing by the collector, on the other.").

103. Sunstein, *supra* note 24, at 216.

104. *Id.* at 217.

105. *See* Joel Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1323 (2000) ("While each isolated piece of information may have little meaning or risk minimal potential harm to the individual, the aggregate collection takes on an entirely different character. Analyzing the aggregate can reveal patterns of behavior, profiles, and an intimate slice of the lives of individuals, which can be used to categorize and segregate individuals in society.").

106. Patrick Wintour, *Russian Bid to Influence Brexit Vote Detailed in New US Senate Report*, GUARDIAN (Jan. 10, 2018), https://www.theguardian.com/world/2018/jan/10/russian-influence-brexit-vote-detailed-us-senate-report [perma.cc/4WGK-XYYJ].

online political manipulation.[107] Calling this a crisis of democracy is an understatement.

The dispersed and cumulative nature of online manipulation may point to a collective action problem. Affected individuals or groups may not have an incentive to pursue any form of legal action to redress their harm, but would rather internalize it. This internalization also means that in the absence of any regulation, democracy itself would find it difficult to counter the harms of online manipulation, due to its dispersed and cumulative nature. A solution must account for the collective nature of the harm resulting from online manipulation and its impact on democratic deliberation.[108] Indeed, legal scholars are already exploring many potential legal solutions.[109] Should tort law and class action empower litigants in fighting online manipulation?[110] What kind of government regulation should be imposed on social media and other data aggregators?

But online manipulation has a far more troubling characteristic. The collective nature of its harm stems from its scalability, which affects large volumes of individuals and groups. While manipulation itself predates the Internet, its quantitative escalation could lead to more dangerous consequences for democracy as a whole.[111] This is perhaps best explained by comparing an individual manipulating others in-person to an intelligent technology which makes sense of data and devises ways to manipulate multiple individuals.

Ryan Calo identifies two distinct characteristics that differentiate digital market manipulation from more traditional forms of manipulation—*personalization* and *systemization*.[112] According to Calo, the ability to create personalized advertisements through automated or semiautomated systems is

107. Craig Timberg, *Russia Used Mainstream Media to Manipulate American Voters*, WASH. POST (Feb. 15, 2018), https://www.washingtonpost.com/business/technology/russia-used-mainstream-media-to-manipulate-american-voters/2018/02/15/85f7914e-11a7-11e8-9065-e55346f6de81_story.html?noredirect=on&utm_term=.4dc6ad5a8e27 [perma.cc/9W2E-8FJS].

108. *See, e.g.*, McSweeny, *supra* note 27, at 515 ("For example, millions of fake comments were filed with the Federal Communications Commission during its proceeding revising the Open Internet rules . . . .").

109. *See* Woods, *supra* note 100 (detailing the potential legal responses to Cambridge Analytica).

110. *See* McClurg, *supra* note 37, at 69 (making the case for a new tort to address the dehumanizing and privacy-invasive practice of data profiling).

111. *See generally* Brandon Faulkner, Note, *Hacking Into Data Breach Notification Laws*, 59 FLA. L. REV. 1097, 1098–99 (2007) ("The characteristics of cybercrime have practically eliminated the spatial and temporal restraints that have traditionally limited the quantity of victims and the amount of damages.").

112. Calo, *supra* note 22, at 1021.

itself novel, leading to the "systemization of the personal."[113] The significance lies not in the technology itself, but rather in its impact on human-to-human interactions, which is the main justification for legal intervention.[114]

Political online manipulation could leverage individual weaknesses and unique characteristics to manipulate broader swathes of society and bring about electoral and policy change. Unlike human manipulation, computer program manipulation has "additional advantages over people in that it never tires, has a nearly limitless memory, and can obscure or change its identity at will."[115] These distinct characteristics create a phenomenon that feels different than its predecessor.[116] Perhaps with online manipulation, the challenge also becomes its relationship to *source volume*, from which it benefits. Source volume means that an immense amount of data points, even nonpersonal data, on every aspect of our personalities and activities is available simply as a result of Internet economics and new technologies, which enhances the sophistication of online manipulation.

For example, Jonathan Zittrain writes about a form of online political manipulation he calls "digital gerrymandering."[117] Facebook designed a message that attempted to convince users to vote by showing that their friends had already voted. They believed that this message would convince the average person to vote and that it would increase overall voter turnout. Indeed, Facebook discovered that users who received such message were 0.39 percent more likely to vote.[118] As many as 60,000 individuals decided to vote as a consequence of that tailored message, and the ripple effect brought another 280,000 voters who did not receive the message to the polls.[119] But what if

113. *Id.*

114. *See* Jack Balkin, *The Path of Robotics Law*, 6 CALIF. L. REV. CIR. 45, 48–49 (2015) ("[W]hat lawyers call 'technology' is usually a shorthand for something far more complex. When we talk about 'technology,' we are really talking about (1) how people interact with new inventions and (2) how people interact with other people using those new inventions or presupposing those new inventions.").

115. Calo, *supra* note 22, at 1040.

116. *Id.* at 1022 ("The systemization of the personal may prove different enough from prior selling practices that regulators or courts will seek limits on digital market manipulation, even if they would be hesitant to curtail age-old sales practices like interpersonal flattery. Or, at the very least, digital market manipulation may just feel different enough to justify intervention.").

117. Jonathan Zittrain, Response, *Engineering an Election*, 127 HARV. L. REV. F. 335, 336 (2014) https://harvardlawreview.org/2014/06/engineering-an-election/ [https://perma.cc/93TH-5B9Z] (defining digital gerrymandering as "the selective presentation of information by an intermediary to meet its agenda rather than to serve its users").

118. *Id.* at 336.

119. *Id.*; *see also* John Markoff, *Social Networks Can Affect Voter Turnout, Study Says*, N.Y. TIMES (Sept. 12, 2012), https://www.nytimes.com/2012/09/13/us/politics/social-networks-affect-voter-turnout-study-finds.html [perma.cc/89YP-NB5Z].

Facebook had decided to support one candidate over the other and only serve encouraging messages to certain users who are likely to support a particular candidate? Such manipulation raises a very real question about the boundaries of data use, and while this takes the form of experimentation, it nonetheless endangers democracy. In this hypothetical, data-breach notification law may not offer a remedy, since there is no "breach" that the law is concerned with. However, if Facebook was an information fiduciary, Facebook would be under certain obligations which would classify this data use as a breach of the duty of care and loyalty.

Omri Ben-Shahar critiques today's data economy based on the phenomenon of "data pollution."[120] He argues that construing the harms emanating from data misuse as privacy harms on a very individualistic level[121] is an outdated paradigm because today's data misuse in the form of election interference represents a social harm which affects public interests more than it affects individual privacy.[122] Ben-Shahar equates this phenomenon to pollution, because emission of data in such harmful ways creates externalities for society at large, representing a failure of private law and suggesting that we may need a legal solution similar to environmental protection law.[123]

2. Experimentation

Several scholars also note that manipulation, at least at this point in time, leads to experiments on human subjects.[124] This may seem like a farfetched concern, but Facebook and Cornell University researchers engaged in a covert mood manipulation experiment back in 2012.[125] Through an algorithm,

120. Omri Ben-Shahar, *Data Pollution* 1–51 (U. of Chi. Pub. Law, Working Paper No. 679, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3191231 [perma.cc/P462-Z4UD].

121. *Id.* at 3 ("Under the privacy paradigm, the collection of personal data creates various harms to the *individuals* whose data is collected, used, shared, or lost.").

122. *Id.* at 7–10.

123. *Id.* at 7 ("[One approach to pollution control is] to utilize ex-post devices, to be triggered in the aftermath of harmful data emissions. Like toxic waste releases from industrial production, data spills are rapidly becoming a major social problem of the digital era. Environmental law uses various tools to shift the harm from toxic waste to the emitters, and data pollution law could similarly focus on liability and prevention. While cleanup of spilled data is largely impossible, the harm from the release can be mitigated by post-spill actions and adequate preparedness. And the expected harm can be reduced by a proper system of deterrence. Liability equal to the social cost of spills (punctuated by compulsory liability insurance) would lead to better precautions and self-regulation.").

124. *See* Zarsky, *supra* note 85, at 175 ("Yet a third way to articulate the manipulation-based argument is to note that such actions are unacceptable as they amount to human experimentation."); *see also* Tamara Piety, *Advertising as Experimentation on Human Subjects*, 19 ADVERT. & SOC'Y Q. (2018).

125. *See* Adam D.I. Kramer et al., *Experimental Evidence of Mass-scale Emotional Contagion*

Facebook altered the feeds of hundreds of thousands of unwitting users. The users were selected at random to have their feed either display more positive or more negative content.[126] Those whose feeds displayed more positive content were more likely to be positive in their status updates, and vice versa.[127] Therefore, this study demonstrated that social media is able to influence the emotional state of its users by affecting the kind of content they get to see.[128] Though commentators believe that it is not illegal to conduct such experiments, there is a strong allegation that this breached ethical research guidelines by not obtaining proper consent from the experiment subjects (randomly selected Facebook users).[129]

Tamara Piety explains that allowing cutting-edge psychological and technological tools in advertisement is a de facto authorization of "widespread experimentation on human subjects without their consent and with only minimal oversight."[130] Piety contends that experimentation on human subjects through online manipulation exposes the subjects to harm.[131] Indeed, manipulation could cause a variety of societal and individual harms—including fear, anxiety, guilt, addiction, sexism, and racism—depending on what data points are exploited.[132] Despite this, online manipulation is largely experimental and not controlled by current regulation.[133] In some cases, these harms may be difficult to show. Nevertheless, even where harm cannot be directly identified beyond a reasonable doubt, online manipulation should still be regulated because such conduct is wrongful and is likely to cause these harms.

Tal Zarsky notes that the strength of the experimentation argument is that it is deontological, meaning that the act of subjecting unwitting humans to an

---

Through Social Networks, 111 PROC. NAT'L ACAD. OF SCI. 8788 (2014).

126. *Id.* at 8789.

127. *Id.* ("[F]or people who had positive content reduced in their News Feed, a larger percentage of words in people's status updates were negative and a smaller percentage were positive. When negativity was reduced, the opposite pattern occurred.").

128. *Id.* ("These results suggest that the emotions express by friends, via online social networks, influence our own moods . . . providing support for previously contested claims that emotions spread via contagion through a network.").

129. *See* Charles Arthur, *Facebook Emotion Study Breached Ethical Guidelines, Researchers Say*, GUARDIAN (June 30, 2014), https://www.theguardian.com/technology/2014/jun/30/facebook-emotion-study-breached-ethical-guidelines-researchers-say [perma.cc/L3EB-3CWK].

130. Piety, *supra* note 124.

131. *Id.*

132. *See id.*

133. *See, e.g.*, Michelle Meyer, *Everything You Need to Know About Facebook's Controversial Emotion Experiment*, WIRED (June 30, 2014), https://www.wired.com/2014/06/everything-you-need-to-know-about-facebooks-manipulative-experiment/ [perma.cc/U9LQ-VG3F] (explaining that Facebook's research is not covered by federal research regulations).

experiment is wrongful in itself. This is because it disrespectfully treats humans as instruments employed to achieve a certain goal.[134] Therefore, it is immaterial whether the experiment is successful, unsuccessful, harmful, or harmless. Though humans have been experimental subjects in many covert projects before, both governmental and corporate, the fact that manipulation is becoming personalized and systemized means that this emerging form of experimentation may be uniquely wrongful.[135] More empirical evidence of direct harms caused by personalized manipulation experiments is likely to emerge, and it may be that the many harms associated with such activity will largely outweigh the benefits.[136]

C. THE EXCEPTIONALISM OF ONLINE MANIPULATION

The exceptional nature of online manipulation has been explored thoroughly in the advertising sector.[137] Ryan Calo, exploring the concept of market manipulation, was concerned with whether this phenomenon is different from offline manipulation, and whether this difference warrants legal intervention.[138] It is important to remember that Calo's analysis of market manipulation is slightly different from other forms of online manipulation, since marketing is largely focused on methods of convincing potential customers to purchase goods and services. Therefore, the effects of market manipulation would be, at most, some loss of privacy, consumers paying for products they do not need, or paying extra for a certain brand.[139] On the individual consumer level, the cost or harm is marginal. This explains why regulators, such as the Federal Trade Commission, have not attempted to address market manipulation.[140]

The availability of data on every aspect of our existence exacerbates this scalability and facilitates it. Today, an ever-increasing breadth of personal data is collected by different actors. Social media is learning about our personalities and preferences by looking at what we share and "like,"[141] shopping platforms

134. *See* Zarsky, *supra* note 85, at 175.

135. *See id.* at 175 (calling this form of experimentation "socially unacceptable").

136. *See id.*

137. *See generally* Tal Zarsky, *Online Privacy, Tailoring, and Persuasion*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION 209–24 (Katherine Strandburg & Daniela Stan Raicu eds., 2006).

138. *See* Calo, *supra* note 22, at 1020–24.

139. *See id.* at 1024–34.

140. *See id.* at 1002 ("One reason why market manipulation may not have received sustained scrutiny is that its effects, while pervasive, are limited. Maybe a consumer pays a little extra for a product, for instance, or purchases an item on impulse. Thus, both the downside for consumers and, importantly, the upside for firms, have proven only marginal to date.").

141. *See, e.g.*, Carole Cadwalladr & Emma Graham-Harrison, *How Cambridge Analytica Turned Facebook "Likes" Into a Lucrative Political Tool*, GUARDIAN (Mar. 17, 2018),

are tracking our habits and purchasing patterns,[142] and sensor-based gadgets—"the Internet of Things"—are collecting data about us and our environments.[143] Household items including smartwatches, vehicles, thermostats, locks, refrigerators, and medical devices all collect personal data.[144] The Internet of Things enhances the ability to collect such a vast and rich volume of data points, which are unique in the sense that regular Internet use would not generate the same quantity of sensor data collected by refrigerators, smart watches, thermostats, and so on. This personal information and sensor data about us could provide a very intimate insight into our lives and open it up for abuse, especially as companies like Facebook, Google, and Twitter are selling their user data to third parties.[145] The large volumes of quality sensor data also create an unprecedented ability to better micro-target individuals.[146] As such, this form of nearly flawless microtargeting is far more intrusive and manipulative than ever before, suggesting that it may become fairly easy to manipulate individuals based on an aggregation of data available about every aspect of their lives.

This may be the moment where legal intervention is going to be more necessary than ever before. As Daniel Solove observes, the dynamic nature of the Internet provides much better targeting capabilities as opposed to static

---

https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm [https://perma.cc/D6NL-T5W5] (arguing that "likes" are valuable data that could be utilized for manipulation).

142. *See, e.g.*, Michael Reilly, *Google Now Tracks Your Credit Card Purchases and Connects Them to Its Online Profile of You*, MIT TECH. REV. (May 25, 2017), https://www.technologyreview.com/s/607938/google-now-tracks-your-credit-card-purchases-and-connects-them-to-its-online-profile-of-you [perma.cc/2Y8R-ST5K]; *see also* Solove, *supra* note 33, at 1411. *But see* Joseph Phelps et al., *Privacy Concerns and Consumer Willingness to Provide Personal Information*, 19 J. PUB. POL'Y & MARKETING 27, 27 (2000) (arguing that the high level of consumer privacy concern appears to have had little discernible impact on consumers' shopping behaviors, as most consumers are willing to give up some of their privacy to participate in a consumer society).

143. *See generally* Bruce Schneier, *Security and the Internet of Things*, SCHNEIER ON SECURITY (Feb. 1, 2017), https://www.schneier.com/blog/archives/2017/02/security_and_th.html [perma.cc/SAU3-UR94].

144. *See* Ido Kilovaty, *Freedom to Hack*, 80 OHIO ST. L.J. 455, 472 (2019) ("IoT devices enable not only data about direct computer use but also data about driving, home heating and cooling, food stored in a refrigerator, pulse and blood pressure, sleep patterns, and much more.").

145. *See, e.g.*, González, *supra* note 22, at 9.

146. *See, e.g.*, Sara M. Watson, *Russia's Facebook Ads show how Internet Microtargeting can be Weaponized*, WASH. POST (Oct. 12, 2017), https://www.washingtonpost.com/news/posteverything/wp/2017/10/12/russias-facebook-ads-show-how-internet-microtargeting-can-be-weaponized/?utm_term=.95eb1222ab96 [perma.cc/YJW4-MZLQ] (explaining how Russian operatives used algorithms and past behavior to predict and exploit Facebook users' desires and inclinations in the 2016 U.S. presidential election).

mediums like television or magazines.[147] Solove was concerned about the use of targeting for marketing, yet these techniques have now made it into politics as well. This distinct quantitative nature of online manipulation calls for a novel qualitative approach.[148]

But consider the following scenario. Online manipulation is far more sophisticated than its offline counterpart, because the offline form is limited by physics, information gaps, and lack of scalability. A salesperson would face limits in the offline world, as she does not know enough about the potential consumer and her personality, she cannot change her own appearance, and she has limited ability to gain trust.[149] However, online manipulation does not have these limitations.

Data obtained in data breaches may facilitate financial fraud, but the same data may also be used for non-financial online manipulation. While certain financial information like credit card numbers could be easily replaced by financial institutions after a breach, this is not the case for personal information misused for manipulation purposes, particularly if such information reflects immutable or quasi-immutable characteristics like sexual orientation, race, nationality, ideology, and more. Since the Internet does not forget, personal data needs a far more protective legal regime to avoid irreversible and long-lasting harm to privacy and autonomy.[150] Needless to say,

147. Solove, *supra* note 33, at 1410 ("This revolution in targeting technology is possible because web pages are not static like magazine pages. They are generated every time the user clicks. Each page contains spaces reserved for advertisements and specific advertisements are download into those spots. The dynamic nature of web pages makes it possible for a page to download different advertisements for different users. Targeting is very important for web advertising because a web page is cluttered with information and images all vying for the users' attention. Whereas a television commercial is an orderly linear presentation of details, the web page places everything before the user at once.").

148. In legal literature, increased quantity often affects the qualitative analysis and approach. For example, a similar approach was discussed in the context of Fourth Amendment doctrine, analyzed by Orin Kerr in the aftermath of *United States* v. *Jones*. *See* Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012). There, Justice Alito's concurring opinion suggested that for Fourth Amendment purposes, "long-term GPS monitoring of a car counts as a search even though short-term monitoring does not," supporting what is called "the mosaic theory." *Id.* at 313.

149. *See* Calo, *supra* note 22, at 1021.

150. *See* Solove, *supra* note 33, at 1412–13 ("As we live more of our lives on the Internet, we are also creating a permanent record of unparalleled pervasiveness and depth. Indeed, almost everything on the Internet is being archived . . . . Our online personas—captured, for instance, in our web pages and usenet postings—are swept up as well. . . . But little on the Internet disappears or is forgotten, even when we delete or change the information. The amount of personal information archived will only escalate as our lives are increasingly digitized into the electric world of cyberspace."); *see also* Solove & Citron, *supra* note 33, at 758–59 ("The problem with identity theft is that personal data cannot readily be 'cancelled' like a credit-card number. Social Security numbers are difficult to change. Other personal data

such illegally obtained data is often widely available on the dark web,[151] allowing any potential manipulator to obtain that data and misuse it accordingly.[152] Currently, cybersecurity law provides for remedies relating to financial information, but ignores the emerging forms of data misuse which can be just as threatening, if not more so.

III. DATA-BREACH LAW: SILVER LININGS AND GAPS

Data-breach notification law comprises a patchwork of federal and state statutes that impose a duty to notify affected individuals when their personal information has been compromised.[153] When a system is breached, the breached entity is required to send out notifications to consumers in accordance with the different state data-breach notification laws. By requiring breached entities to inform consumers, the law enables those affected to mitigate the risks associated with the data leak by pursuing a course of action they deem appropriate or necessary.[154] Creating that sort of public awareness

---

such as birth date and mother's maiden name cannot be replaced. Biometric data such as fingerprints or eye scans, health information, and genetic data cannot be exchanged. A criminal may obtain a victim's personal data and use it months or years later; the data will still be useful for committing fraud.").

151. Personal information obtained in data breaches is often sold on websites on the dark web—a section of the internet only accessible with specialist software such as the TOR browser. This personal information most often includes credit card numbers, social security numbers, and financial information, but it may also be information of other kind that can facilitate non-financial manipulation. *See, e.g.*, Kate O'Flaherty, *93 Million Accounts Exposed as Third Data Trove Goes on Sale on the Dark Web*, FORBES (Feb. 18, 2019), https://www.forbes.com/sites/kateoflahertyuk/2019/02/18/another-93-million-accounts-exposed-as-third-data-trove-goes-on-sale-on-the-dark-web/#2c5f8d521706 [perma.cc/RKA3-3GUQ].

152. *See, e.g.*, Alyssa Newcomb, *Your Identity Is for Sale on The Dark Web for Less Than $1,200*, NBC NEWS (Mar. 12, 2018), https://www.nbcnews.com/tech/security/your-identity-sale-dark-web-less-1-200-n855366 [perma.cc/W89Z-AU6V]; *see also, e.g.*, Tomáš Foltyn, *Babies' Personal Data Hawked on Dark Web*, WELIVESECURITY (Jan. 26, 2018), https://www.welivesecurity.com/2018/01/26/babies-personal-data-dark-web/ [perma.cc/A4EW-MRDS].

153. Federal data-breach notification law includes statutes like Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act. State data-breach notification law includes all state statutes on the mandatory disclosure of a data breach affecting residents of that state. *See* Sara A. Needles, *The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law*, 88 N.C. L. REV. 267, 272 (2009); *see generally* Karl D. Belgum, *Who Leads at Half-Time?: Three Conflicting Visions of Internet Privacy Policy*, 6 RICH. J.L. & TECH. 1, 24 (1999); *see also* Kosseff, *supra* note 9, at 1011 (creating six categories for the patchwork of federal and state statutes: "(1) data security statutes; (2) data breach-notification statutes; (3) data security litigation through common law and statutory claims; (4) computer hacking laws; (5) electronic surveillance laws; and (6) the Cybersecurity Act of 2015").

154. *See* Needles, *supra* note 153, at 24.

is immensely important in an area where secrecy and ambiguity are rampant. This is but one area covered by what is often referred to as "cybersecurity law." Data-breach notification law is used as a case study in this Article, as it represents a microcosm of the different tradeoffs, interests, values, and balances that underlie cybersecurity law.

Under this scheme, residents of different states—California, New York, Texas, and others—will be covered by their own respective statutes, which often differ in some respects.[155] For example, the California statute provides that a breached entity should provide the following sections in the notification—"What Happened," "What Information Was Involved," "What We Are Doing," and "What You Can Do."[156] However, many other states have no corresponding provision, which could affect whether a notification is effective in dealing with the risk of future manipulation if such sections are not mandated.[157]

In the context of manipulation, the law suffers from definitional and substantive shortcomings. These concerns are specific to data-breach notification law, but they can also be found across federal and state statutes and regulations dealing with information security.

The definitional shortcoming is fairly straightforward. Data-breach notification law limits its applicability to compromised *personal information* resulting from a *breach of security*. Since each state has its own statute, these definitions usually vary, but the concepts of *personal information* and *breach* often overlap across many states. This was intended to ensure that only certain irregular events are covered by the law, while others would be outside of the scope of the law's applicability. It perhaps made sense at the time to provide this limit, but advancements in technology, paired with new forms of data abuse, creates an uneasy reality of impunity in the wake of emerging technologies. In fact, many privacy laws revolve around similar delineations, which creates a systemic vulnerability when it comes to addressing online manipulation.[158]

155. For a comparison of all state breach notification laws as of July 1, 2019, see *State Data Breach Notification Laws*, FOLEY & LARDNER LLP (July 1, 2019), https://www.foley.com/en/insights/publications/2019/01/state-data-breach-notification-laws [https://perma.cc/ZFB9-AGGR].

156. CAL. CIV. CODE § 1798.29(d)(1) (West 2019); CAL. CIV. CODE § 1798.82(d)(1) (West 2019).

157. For example, the Texas statute does not have a corresponding provision. *See* Identity Theft Enforcement and Protection Act, TEX. BUS. & COM. CODE ANN. §§ 521.001–.152, (West 2017).

158. *See generally* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

On the substantive level, data-breach jurisprudence only takes issue with tangible harms stemming from identity theft or fraud. For example, the Supreme Court held that plaintiffs in data-breach litigation need to prove "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."[159] Since then, the Courts of Appeals remain divided on the question of harm. Some Circuits recognize that an increased risk of future harm is sufficient to satisfy Article III standing.[160] However, at least two Circuits do not recognize future risk of harm as sufficient for standing.[161] While the Supreme Court had the opportunity to resolve this circuit split in a petition for writ of certiorari in the matter of *Zappos.com, Inc.* v. *Stevens*,[162] it refused to do so and denied the petition.[163]

Along similar lines, the vast majority of state statutes call for a risk-of-harm analysis to determine whether a notification is required under the respective state statute.[164] If there is no risk of harm (usually defined as financial or identity theft harm), the notification requirement is not triggered. While financial fraud and identity theft still represent serious social problems, this approach significantly impedes what data-breach notification law could do in response to online manipulation as well as other serious harms. It is crucial to understand these definitional and substantive difficulties as part of one whole system and contrast them with the growing concerns and phenomena

159. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1543 (2016) (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)).

160. *See, e.g.*, Galaria v. Nationwide Mut. Ins. Co., 663 Fed. Appx. 384 (6th Cir. 2016) (holding that increased risk of fraud and identity theft resulting from insurer's negligent conduct are sufficient to create standing); Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016) (holding that increased risk of fraudulent charges and identity theft are future injuries sufficient to satisfy Article III standing); Resnick v. AvMed, Inc., 693 F.3d 1317 (11th Cir. 2012) (holding that claims of identity theft resulting from data breach are sufficient to create Article III standing).

161. *See* Whalen v. Michaels Stores, Inc., 689 Fed. Appx. 89 (2d Cir. 2017); Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017).

162. *In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., 888 F.3d 1020 (9th Cir. 2018), *petition for cert. filed sub nom.* Zappos.com, Inc. v. Stevens, 87 U.S.L.W. 3065 (2018) (No. 18-225).

163. Greg Stohr, *Amazon Zappos Rejected by U.S. Supreme Court on Data Breach Suit*, BLOOMBERG (Mar. 25, 2019), https://www.bloomberg.com/news/articles/2019-03-25/amazon-s-zappos-rejected-by-u-s-high-court-on-data-breach-suit [perma.cc/67K3-M7VJ].

164. *See* BAKER HOSTETLER, DATA BREACH CHARTS (2018), https://www.bakerlaw.com/files/uploads/documents/data%20breach%20documents/data_breach_charts.pdf [perma.cc/9TGQ-APDP] (demonstrating that as many as forty-three state statutes require some form of risk-of-harm analysis to determine whether the notification requirement is triggered).

associated with online manipulation.

A. DEFINITIONAL BOUNDARIES

State data breach notification laws typically revolve around two important definitions. First, whether the compromised information in question is *personal information*, as defined in the statute, and, second, whether the event in question is covered by the statute, i.e., whether it is in fact a *data breach* or *breach of security* as provided in the respective statute.

1. Personal: Demographic Versus Psychographic

Different federal and state statutes on information security and privacy contain their own definitions of "personal information." Data breach notification laws have their respective definitions in each state,[165] as well as in federal legislation such as the Children's Online Privacy Protection Act,[166] Financial Modernization Act,[167] Fair Credit Reporting Act,[168] Health Insurance Portability and Accountability Act,[169] and the Privacy Act.[170] The definition of "personal information" is similar under each of these legislative regimes in

165. *See, e.g.*, CAL. CIV. CODE § 1798.29 (West 2019) (defining personally identifiable information as:

> [an] individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
> (1) Social security number.
> (2) Driver's license number or California Identification Card number.
> (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
> (4) Medical information.
> (5) Health insurance information).

166. 15 U.S.C. § 6501(8) (2018); 16 C.F.R. § 312.2 (2019) (defining "personal information" as "individually identifiable information about an individual collected online" which among other things, includes first and last name, home address, e-mail address, telephone number, and Social Security number).

167. 15 U.S.C. § 6809(4)(A) (2018) (defining "nonpublic personal information" as "personally identifiable financial information").

168. 15 U.S.C. § 1681a(d)(1) (2018) (defining "consumer report" as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living").

169. 45 C.F.R. § 160.103 (2019) (defining "protected health information" as "individually identifiable health information").

170. 5 U.S.C. § 552a (1976) (defining "record" as a combination of "education, financial transactions, medical history, and criminal or employment history" and the employee's "name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph").

their focus on demographics and plainly identifiable information about the individuals covered by their mandate.

The focus on demographic information as personal information is understandable, as these statutes were enacted long before advanced technologies made psychographic profiling possible. However, today, the tension between demographics and psychographics is very well demonstrated by this narrow approach adopted by data-breach notification law, focusing on whether personal information was accessed or not. It is now obvious that this approach is fundamentally flawed. This is not to say that the protection of demographic information is not important for society as a whole. Rather, data that does not qualify as "personal information" under the law could nonetheless be misused if accessed by unauthorized actors. These actors can then process that data through advanced technologies similar to Cambridge Analytica, which leveraged thousands of data points it obtained on millions of individuals whose information was compromised. As Andrew McClurg aptly put it in this context—"a thousand words are . . . worth a picture."[171] Many tiny data points may create a highly detailed picture about an individual's life. Jeff Kosseff notes that such nonpersonal information "still may be quite sensitive and valuable to identity thieves or other criminals, but the notification rule does not apply."[172] Andrea Matwyshyn holds a similar view, in which she argues that legally sensitive information is not necessarily the most valuable kind of information. She argues "[v]alue in information is driven by scarcity, not sensitivity."[173] For example, our credit card information may be sensitive, but it is not scarce because of how often we share that information with businesses and other individuals. However, an ice cream preference may not be as sensitive, but it is scarce.[174] After all, how often is that information provided to others? The value of the latter, therefore, may be much higher than a replaceable credit card number.[175] This represents a considerable gap between how the law views sensitive information worthy of protection and

171. McClurg, *supra* note 37, at 70.

172. JEFF KOSSEFF, CYBERSECURITY LAW 37–38 (2017).

173. Andrea M. Matwyshyn, *Privacy, The Hacker Way*, 87 S. CAL. L. REV. 1, 15 (2013).

174. *Id.* at 25 ("Perhaps the most essential part of finding value in access to information about my favorite beer and my network of friends, however, rests in its scarcity. The fewer the number of people who know the name of my favorite beer and the identities of my friends, the fewer the number of companies that can market to us with an informational edge. In other words, access to the knowledge of my favorite beer involves information that is subject entirely to my control and derives independent value from not being widely known.").

175. *See* Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Apr. 9, 2018), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ [perma.cc/NJ9Z-5EMT] (reporting that credit card numbers sell for a relatively cheap price on the dark web, ranging from $5–$110).

non-sensitive or nonpersonal information that is excluded from its scope.

These notions are further strengthened by Paul Ohm's contention that computer science has demonstrated the capability to "reidentify" and "deanonymize" databases of anonymized personal information.[176] What this means is that our understanding of what constitutes personal and nonpersonal, encrypted and decrypted, and anonymized and deanonymized is immensely outdated. The peril in such anachronism is that a considerable portion of current information privacy law is outdated and dangerously ineffective, requiring a reexamination by lawmakers.[177]

Paul Schwartz and Daniel Solove highlighted a similar problem, which they called the Personally Identifiable Information (PII)[178] problem.[179] They determine that the "unstable category" of PII adopted by information privacy law is flawed because it limits the scope of what information is worthy of legal protection.[180] PII is not a category limited to just one statute—rather, it is an overarching theme in all of information privacy and security law, both on the federal and state levels.[181] They conclude that the delineations of PII and non-PII should not be abandoned, but instead recommend certain modifications to the PII approach, calling it PII 2.0. PII typically includes information such as first and last name, address, work telephone number, email address, home telephone number, and general educational credentials.[182] This definition still excludes psychographics—personality traits, weaknesses, tendencies, affiliations, and more.

2. Breach Versus Unauthorized Acquisition

The definition of "breach of security" in most state data-breach notification laws is based on unauthorized acquisition of personal information.[183] Like many other state statutes, the California statute defines breach of system security as "unauthorized acquisition of computerized data

176. *See* Ohm, *supra* note 158, at 1704.

177. *See id.* ("Yet reidentification science exposes the underlying promise made by these laws—that anonymization protects privacy—as an empty one, as broken as the technologists' promises. At the very least, lawmakers must reexamine every privacy law, asking whether the power of reidentification and fragility of anonymization have thwarted their original designs.").

178. *See* 2 C.F.R § 200.79 (2019) ("PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.").

179. Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1836 (2011).

180. *Id.* at 1816.

181. *Id.*

182. *See* 2 C.F.R. § 200.79 (2019).

183. *See, e.g.*, CAL. CIV. CODE § 1798.29 (West 2019); *see also* JOHN HUTCHINS ET AL., U.S. DATA BREACH NOTIFICATION LAW: STATE BY STATE (2007).

that compromises the security, confidentiality, or integrity of personal information maintained by the agency."[184] Similarly, the U.S. Computer Emergency Readiness Team (US-CERT) defines data breach as the "unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information."[185] However, these statutes should focus on the data compromised, rather than whether an intrusion took place or not. Sara Needles observes that data-breach notification laws apply to a broad set of activities that compromise personal information.[186] A few examples include the physical loss of hardware (such as laptops and USB drives), an individual unintentionally misusing data, insider threat, a vendor inappropriately authorizing use of data, or an external intrusion.[187] This notion makes a lot of sense, considering that the purpose behind the law is to inform consumers that their data is now in the possession of an unauthorized entity. After all, stolen laptops containing sensitive information are not much different than hacking those same laptops.[188]

However, many companies have resisted a broader understanding of activities that would trigger data-breach notification laws. These companies push for an interpretation that asks whether an external intrusion—a "hack"—took place.[189] This means that many compromised companies would not be required to inform consumers affected by the data loss unless there is an external actor who intruded on digital assets that include unencrypted personal information.[190]

184. CAL. CIV. CODE § 1798.29(f) (West 2017).

185. *See Glossary*, US-CERT (Nov. 28, 2018), https://niccs.us-cert.gov/glossary [perma.cc/4K76-T58H] (defining data breach as "[t]he unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information").

186. *See* Needles, *supra* note 153, at 274 (listing the many aforementioned examples of data breaches).

187. *Id.*

188. *See, e.g.*, *id.* (noting that the Bureau of Alcohol, Tobacco, Firearms, and Explosives lost hundreds of laptops between 2002 and 2007, many containing classified or sensitive data).

189. *See* Ido Kilovaty, *The Cambridge Analytica Debacle is Not a Facebook "Data Breach." Maybe it Should Be*, TECHCRUNCH (Mar. 17, 2018), https://techcrunch.com/2018/03/17/the-cambridge-analytica-debacle-is-not-a-facebook-data-breach-maybe-it-should-be [perma.cc/P6UE-HDHG] ("There was no unauthorized external hacking involved, meaning that Facebook databases were not breached by an outside malicious actor. At the same time, this approach misses the point entirely in terms of user privacy and security. It should not matter for a company like Facebook whether their users' personal information was forcefully obtained through brute-force, or whether Facebook's personnel were manipulated to hand in that information to malicious and untrustworthy party.").

190. *See* Lorenzo Franceschi-Bicchierai, *Why We're Not Calling the Cambridge Analytica Story a 'Data Breach'*, MOTHERBOARD (Mar. 19, 2018) https://motherboard.vice.com/

This leads to a paradox. The incentives and disincentives provided by information privacy and security law results in malicious actors gaining access to personal information through lawful channels. For example, malicious actors can purchase data or access it through developer-facing platforms.[191] This was the case with Cambridge Analytica: even though it purchased the data collected by Facebook, it did so by contacting a developer who had a direct and legitimate channel between his app and Facebook's *Graph* API.[192] While the actions of Cambridge Analytica did not constitute a breach in the technical sense, as they did not hack or attempt to hack Facebook, it nonetheless was a breach of security in the consequential sense. This is because personal and nonpersonal data about certain Facebook users made its way to unauthorized hands.[193] This is an important distinction to keep in mind, as Facebook vehemently denied that there was a data breach in the legal or technical sense by claiming that Cambridge Analytica's unauthorized access to Facebook data "was unequivocally not a data breach" as "no passwords or information were stolen or hacked."[194] Strategically, it is clear why Facebook chose that rhetorical path, as the regulatory and public-relations' implications of admitting a breach for any company are staggeringly significant,[195] though Facebook still notified

en_us/article/3kjzvk/facebook-cambridge-analytica-not-a-data-breach [perma.cc/W3ET-RDKG] ("[W]e believe that describing this incident as a breach would . . . mislead our readers . . . . No one hacked into Facebook's servers exploiting a bug, like hackers did when they stole the personal data of more than 140 million people from Equifax. No one tricked Facebook users into giving away their passwords and then stole their data, like Russian hackers did when they broke into the email accounts of John Podesta and others through phishing emails.").

191. *See* Nicholas Thompson & Fred Vogelstein, *A Hurricane Flattens Facebook*, WIRED (Mar. 20, 2018), https://www.wired.com/story/facebook-cambridge-analytica-response/ [perma.cc/DK8E-W8A8] ("The story of how Kogan ended up with data on 50 million American Facebook users sounds like it should involve secret handshakes and black hats. But Kogan actually got his Facebook data by just walking in Facebook's front door and asking for it. Like all technology platforms, Facebook encourages outside software developers to build applications to run inside it, just like Google does with its Android operating system and Apple does with iOS."); *see also* Kilovaty, *supra* note 189.

192. Jonathan Albright, *The Graph API: Key Points in the Facebook and Cambridge Analytica Debacle*, MEDIUM (Mar. 20, 2018), https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747 [perma.cc/NBV2-VJNG] ("Facebook's Graph API was a revolution in large-scale data provision. It converted people and their likes, connections, locations, updates, networks, histories, and extended social networks into — quite literally — 'objects.' It made the company's offerings and the data its users generated more economically viable.").

193. *See* Kilovaty, *supra* note 7.

194. *See* Andrew Bosworth (@boztank), TWITTER, (Mar. 17, 2018, 7:38 AM), https://goodyfeed.com/wp-content/uploads/2018/03/fb-3.png [perma.cc/UG3M-VV66].

195. *See* Kate Vinton, *Is It Time to Force Companies to Admit When They've Been Hacked?*, FORBES (June 11, 2014), https://www.forbes.com/sites/katevinton/2014/06/11/is-it-time-to-force-companies-to-admit-when-theyve-been-hacked/#4c7330c5f67a [https://perma.cc/

its users after the incident was reported by the press.[196]

Julie Cohen emphasizes how third parties that gain unauthorized access to data are able to use it in ways that are anything but transparent.[197] She says:

> Most reputable firms that deal directly with consumers do disclose some information about their 'privacy practices,' but the incentive is to formulate disclosures about both purposes and potential recipients in the most general terms possible. This practice shields secondary recipients of personal data, many of whom do not disclose information about their activities at all.[198]

What Cohen means is that while regulators tend to focus their efforts on primary data collectors, such as Facebook and Google, it is often the secondary use of data that lacks transparency and therefore harms the data subjects in uncontrollable ways. This was best exemplified by Facebook (primary data collector) sharing data with Aleksandr Kogan (secondary recipient) who transferred that data to a third party: Cambridge Analytica.

In a sense, data-breach notification law makes the primary data collector solely responsible for data misuse. In some respects, the primary data collector is better situated to provide the transparency and information on what is being done with the data, and more importantly, whether there is a risk or actual occurrence of manipulation down the line. For example, a social media platform whose data is compromised would be able to learn more about the risks, how such data is being misused, and who the perpetrator is, especially as the legal dispute and potential investigation emerges between regulators, social media, and the unauthorized entity. At times, regulatory agencies such as the FTC and SEC may step in with enforcement action, but the expectation is that the collector of the data notify its users of any abnormalities.

B. SUBSTANTIVE SHORTCOMINGS

A major substantive shortcoming in current cybersecurity law, primarily in how it is litigated, is its narrow focus on identity theft as a harm.[199] It is hard

B8XN-U56X] ("Embarrassment and business culture contribute to a lack of transparency in data breach reporting, according to Boyer. The majority of security breaches are accomplished through less-than-sophisticated methods, and companies don't like admitting to these kinds of attacks.").

196. Steve Inskeep, *Facebook Will Notify 87M Users Whose Data May Have Been Used By Cambridge Analytica*, NPR (Apr. 5, 2018), https://www.npr.org/2018/04/05/599997683/facebook-will-notify-87m-users-whose-data-may-have-been-used-by-cambridge-analyt [perma.cc/WL8H-5YFX].

197. JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 235 (2012).

198. *Id.*

199. *See* Kosseff, *supra* note 14, at 344–45 ("The current patchwork of laws that purport

to imagine a connection between massive online manipulation and identity theft, as the former does not typically lead to the latter. Manipulating Internet users does not require stealing their identity; it simply denotes that particular information about them is being used against them, and identity misrepresentation certainly is not required. This means that in order for data-breach laws to protect consumers and inform them about potential misuse of their personal data by third parties, it needs to expand its purpose to also protect from the risk and harm of manipulation.

1. Identity Theft Versus Manipulation Harm

The tension between identity theft and manipulation harm is key to understanding why current cybersecurity law fails to protect consumers from the new threats of the digital medium. It is perhaps best illustrated by how, in thirty-eight states, companies are not required to inform their consumers of a breach if they determine that there is no risk of harm.[200] But in that context, what is harm?[201] Most data-breach case law narrowly focuses on the harm of identity theft and fraud, and therefore "risk for harm" relates solely to identity theft and fraud.[202] On that same note, courts have been restrictive in the type of injury that they are willing to recognize and redress as part of data-breach litigation. There may be times where data obtained through a data breach may be used both for identity theft and manipulation, though some data could be insufficiently specific for identity theft, but sufficient to successfully manipulate an individual.

---

to address cybersecurity are focused largely on preventing economic harms such as identity theft.").

200. *See* KOSSEFF, *supra* note 172, at 39 (2017) ("In thirty-eight of the states with breach notification laws, companies can avoid notification obligations if, after investigating the breach, they determine that the incident did not create a risk of harm for individuals whose personal information was exposed.").

201. For a brief theory of harm discussion, see Catherine Padhi, *Standing in Data-Breach Actions: Injury in Fact?*, LAWFARE (Dec. 18, 2017), https://www.lawfareblog.com/standing-data-breach-actions-injury-fact [perma.cc/2DVC-XM4E]. For how the Federal Trade Commission views harm in its data security enforcement action, see Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 639 (2014) ("In evaluating whether a trade practice is unfair, the FTC focuses largely on substantial injury to consumers. Monetary, health, and safety risks are common injuries considered 'substantial,' but trivial, speculative, emotional, and 'other more subjective types of harm' are usually not considered substantial for unfairness purposes."). *See also* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2279 (2015).

202. *See* Priscilla Fasoro & Lauren Wiseman, Covington & Burling LLP, *Standing Issues in Data Breach Litigation: An Overview*, INSIDE PRIVACY (Dec. 7, 2018), https://www.insideprivacy.com/data-security/data-breaches/standing-issues-in-data-breach-litigation-an-overview [https://perma.cc/ZXK8-T38S].

It is understandable why courts follow this path, though this practice is becoming harder to defend. Why are courts unable to recognize manipulation harm as a redressable harm? It is plausible to say that courts do not view online manipulation as a redressable harm due to its ethereal nature. This concern dates back to Nancy Levit's work on "Ethereal Torts," which are "causes of action for intangible or emotional injuries or deprivations of expectancy or reliance interests, the privacy torts, infliction of emotional distress, breach of confidence, breach of good faith, interference with economic expectancies, loss of a chance, or *loss of choice*."[203] In some cases, courts have been able to award damages based on these intangible and emotional injuries.[204] Can a loss of choice be quantifiable for remedy purposes? How about a harm to autonomy, privacy, and democracy?

Legal scholars recognize this inability of courts to grant remedies in cases of privacy harm.[205] In her work, Lauren Scholz argues that privacy should be deemed quasi-property, the violation thereof entitling the victim to restitution, which is the "quintessential privacy remedy."[206] Scholz argues that courts should focus on the defendant's gain when assessing privacy harms.[207] Scholz's work is a demystification of remedies in privacy cases, showing how courts are able to remedy privacy harms. This approach could be extended to remedies in manipulation cases as well, though more scholarly attention would be required for that particular issue.

2. Other Harms

In their seminal article "The Right to Privacy," Samuel Warren and Louis Brandeis recognized that privacy harms may be intangible, but nonetheless be as serious as physical harm.[208] They describe individuals who were subjected to privacy harm as experiencing "mental pain and distress, far greater than could be inflicted by mere bodily injury."[209] So the notion of intangible harm as a result of a privacy harm is not particularly new. Yet, within the rubric of

203. Nancy Levit, *Ethereal Torts*, 61 GEO. WASH. L. REV. 136, 139 (1992).

204. *See, e.g.*, Robert W. Wood, *Hulk Hogan Settles $140 Million Gawker Verdict For $31 Million, IRS Collects Big*, FORBES (Nov. 3, 2016), https://www.forbes.com/sites/robertwood/2016/11/03/hulk-hogan-settles-140-million-gawker-verdict-for-31-million-irs-collects-big/#310b385e6e84 [https://perma.cc/P8WE-SY2U].

205. *See* Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. (forthcoming 2019), https://ssrn.com/abstract=3159746 [perma.cc/KA2D-TE2J].

206. *Id.* at 2.

207. *See id.*

208. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890) ("[M]odern enterprise and invasion have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.").

209. *Id.* at 196.

data-breach litigation, courts tend to favor identity theft harm claims.[210] Recent scholarship suggests that the scope of harms related to data breaches should be reconsidered, and possibly expanded.[211]

Daniel Solove and Danielle Citron recently explored whether harms other than identity theft and fraud should qualify under data-breach notification law.[212] They ask a provocative question: are risk and anxiety harms protected under data-breach notification law? Solove and Citron explain that courts have been consistent in dismissing lawsuits alleging mere risk of identity theft or emotional distress as a consequence of a data breach under Supreme Court precedent set in *Clapper* v. *Amnesty International USA*.[213] In *Clapper*, the plaintiff alleged that government surveillance programs under the Foreign Intelligence Surveillance Act (FISA) harms journalists, lawyers, and human rights activists by requiring them to increase their spending to secure their communications with foreign entities.[214] The *Clapper* Court dismissed the lawsuit on the grounds of lack of standing, holding that plaintiffs did not suffer an "injury in fact" as required under Article III of the Constitution.[215] Solove and Citron note that ever since, courts have held in many cases that the harms alleged were "not concrete or significant enough to warrant recognition."[216] Moreover, even where plaintiffs were able to demonstrate the misuse of their data by hackers, courts have refused to accept such claims as they do not relate to identity theft or future financial injury.[217] However, as demonstrated earlier in this Article, a current circuit split makes Article III standing even more complex and indeterminate.

It should perhaps be a turning point for data-breach notification law, in which we ought to reevaluate what values and interests the law seeks to protect. How can consumers be better informed about the dangers of personal information misuse? And what is the optimal way to reach equilibrium between firms and consumers? Relying solely on narrow dangers such as identity theft and fraud renders legal recourse obsolete in the wake of the advanced technology of manipulation and more nuanced ways to misuse our personal and nonpersonal information.

---

210. *See generally* Solove & Citron, *supra* note 39, at 750 ("The trend is that if a person's personal data has not yet been used to commit identity theft or fraud, then courts find that plaintiffs have suffered no harm.").

211. *Id.* at 756.

212. *Id.*

213. *Id.* at 740.

214. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 406–07 (2013).

215. *Id.* at 422.

216. Solove & Citron, *supra* note 39, at 741.

217. *Id.* at 750.

IV. DATA-BREACH NOTIFICATION LAW AS AUTONOMY-BREACH LAW

While data-breach notification law is primarily concerned with identity theft as a result of unauthorized acquisition of personal information, this law protects a variety of other interests in practice.[218] These interests include reducing risk and uncertainty, and bridging the information gap between firms and consumers.

As firms and malicious actors are better geared today to make sense of big data and to misuse this data for political manipulation through automated systems, the collective magnitude of potential autonomy and privacy harms is far greater than many financial frauds resulting from data breaches. For example, if a data breach leaks primarily financial information, the precautionary steps that need to be taken by all actors are pretty straightforward. Firms inform consumers and strengthen their information security practices, while consumers, with the help of their respective financial institutions, replace compromised credit cards, monitor their credit activity, and report any suspicious activity to the authorities.[219]

The steps to remedy financial data breaches are clear, and for the most part, easily quantifiable. But what should firms and consumers be doing when a data breach has only compromised information that could not be used for financial fraud in any way? This is the murky area of cybersecurity law, which current jurisprudence has not yet fully appreciated. At the very least, breached parties should inform their consumers and provide basic precautionary measures to avoid the adverse effects of manipulation.

At first blush, it may seem that data-breach notification law is a nonobvious solution to the problem of online manipulation. After all, it is essentially a law (or more accurately, fifty state data-breach notification statutes) that addresses when and how companies should inform their consumers of a compromise to their personal information.[220] It requires that breached companies send a notice to affected consumers providing that their data was compromised.

---

218. *See* Needles, *supra* note 153, at 270–71 ("More than simply combating identity theft and economic harm to individuals, many state data breach notification laws strike a balance between the conflicting effects on consumers and businesses. Analyzing what a breach notification portends implicates these two main parties that, in terms of privacy interests, are at odds with one another. Business interests in monetizing data clash against consumer protection groups' cry for data privacy.").

219. Kosseff, *supra* note 9, at 1015 ("Notification requirements might help some customers avoid identity theft and other harms by alerting them of the possible misuse of their personal information.").

220 *See* BAKER HOSTETLER, *supra* note 164.

But data-breach notification law has a greater purpose than that. It directly affects the business model of the digital economy players, who collect data on everyone and everything they interact with. Such massive collection, coupled with the potential harm, raises the question of whether these companies owe certain duties of care, loyalty, and confidentiality to their consumers.

Jack Balkin addresses this exact question.[221] He asks whether online service providers should have special duties to consumers, given that they collect massive amounts of consumer data.[222] His concern is that the intersection of privacy and the First Amendment may make it difficult to regulate this industry, but he offers some potential reconciliations, including treating data as a commodity,[223] which would not trigger the First Amendment because commodities are not speech; and distinguishing between collection, analysis, use, disclosure, and sale of data.[224] He proposes that "many online service providers and cloud companies who collect, analyze, use, sell, and distribute personal information should be seen as information fiduciaries toward their customers and end-users."[225] This means that there would be certain duties attached to information collected by online service providers, which would protect consumers from misuse, disclosure, or other mistreatment of the data collected about them.

In a sense, using data-breach notification law to address online manipulation is an extension of Balkin's concept of information fiduciaries. This is because it provides another mechanism to address data misuse, which forces online actors to comply with certain important duties owed to their consumers should they experience a data breach. As such, applying data-breach notification law to manipulation would result in four primary positive outcomes for consumers.

First, it would reduce information gaps between consumers and online service providers through informative notifications on potential breaches and manipulations. Second, it would indirectly limit what information online service providers would be willing to collect about their users, as any additional data would expose them to the risk of breach, liability, and public relations consequences, such as the one that Uber attempted to avoid in 2016.[226] Third,

221. *See* Balkin, *supra* note 28, at 1186.

222. *See id.*

223. *See id.* at 1195–96.

224. *See id.* at 1196.

225. *Id.* at 1186.

226. Mike Isaac et al., *Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data*, N.Y. TIMES (Nov. 21, 2017), https://www.nytimes.com/2017/11/21/technology/uber-hack.html [https://perma.cc/MFP5-V6DZ] ("Uber disclosed Tuesday that hackers had stolen 57 million driver and rider accounts and that the company had kept the data breach secret for more than a year after paying a $100,000 ransom. . . . The company tracked down the hackers and pushed

it would open an avenue for victims to sue in court, as the identity theft paradigm would be expanded to include manipulation harms. Fourth, it would allow for regulatory oversight, primarily through state attorneys general. While state attorneys general are already investigating manipulation such as Cambridge Analytica, using data-breach notification law to address online manipulation will provide clearer guidelines and concepts to inform their work.

The subsequent Section discusses these four contributions.

A. REDUCING INFORMATION GAPS

The role of reducing the information asymmetry in the context of online manipulation is central to the definition of manipulation. The act of manipulation is almost always hidden,[227] which enables its efficacy. We are often manipulated because we are not aware that we are being deceived or influenced. Manipulation's weakness, therefore, is sunlight.[228] Its disclosure reduces its power.[229] Sunstein acknowledges that the "idea of manipulation is sometimes taken to imply a lack of transparency, as if something important is being hidden or not being disclosed."[230] There is a feature in manipulation that remains hidden, Sunstein says, but once that feature is revealed, the manipulation dissipates.[231] This lack of transparency is an offense to autonomy and dignity.[232]

By disclosing manipulation to potential victims, data holders can preserve or restore individual autonomy and dignity preferably before manipulation even occurs. When companies are breached, and there is a risk of identity theft for their consumers, the law typically requires the company to notify its consumers.[233] After all, the company in question has direct access to breach-

---

them to sign nondisclosure agreements, according to the people familiar with the matter.").

227. The literature recognizes forms of manipulations that are not hidden. *See* Sunstein, *supra* note 24, at 231 ("Some acts can be both manipulative and fully revealed to those who are being manipulated. A graphic health warning, for example, is perfectly transparent (and if it is required by regulation, it is even likely to preceded by a period for public comment, as was the case for the FDA regulation invalidated by *R.J. Reynolds Tobacco Co. v. FDA* (2012)). Subliminal advertising could be preceded by an explicit warning: 'This movie contains subliminal advertising.' If so, it would still count as a form of manipulation.").

228. *See* Romanosky et al., *supra* note 62, at 259 (using the metaphor "sunlight as disinfectant" to refer to disclosure).

229. *Id.*

230. *See* Sunstein, *supra* note 24, at 231.

231. *Id.*

232. *Id.* at 232.

233. *See* Kosseff, *supra* note 9, at 39–40 ("In thirty-eight of the states with breach notification laws, companies can avoid notification obligations if, after investigating the breach, they determine that the incident did not create a risk of [identity theft or fraud] harm for individuals whose personal information was exposed.").

related information that could help consumers reduce the risk of identity theft. The company in question would eventually learn how and who breached their databases, and whether that actor would seek to exploit such data for direct financial gain or for potential manipulation.[234] Regulators, on the other hand, have limited access to such information in the immediate post-breach period. While it is true that a breached company needs to inform regulators of the relevant facts, most of the information related to the breach is in the hands of the breached company. Needless to say, consumers have no knowledge of their own in such a situation, and they rely wholly on what is provided to them by the breached company.

This lack of knowledge and the consumer expectation to be notified is supported by an empirical study carried out by RAND in 2016.[235] In this study, titled "Consumer Attitudes Toward Data Breach Notification and Loss of Personal Information," RAND explored a series of questions relating to the consumer perception and experience with data breaches affecting them.[236] This study asked respondents of the manner in which they learned about a data breach.[237] The study found that as many as fifty-six percent of respondents first learned of a breach by receiving a notification from the affected company.[238] This means that data-breach notification is still a major factor in reducing information gaps between breached companies and their consumers, and it is an important tool in notifying consumers on how their compromised data may be misused against them, though some information gaps are not addressed by data breach notification. Notifications on possible manipulation can "empower consumers to take action to prevent further—or future—harm" and to provide "greater awareness all around."[239] However, additional study is needed to determine what consumers would expect to be notified about.[240]

234. Facebook, for example, did not disclose the fact that Cambridge Analytica misused user data for manipulation. It only became clear that millions of Facebook users' personal data was compromised after a whistleblower, formerly working with Aleksandr Kogan, blew the whistle on the scandal to its full extent. *See* Cadwalladr & Graham-Harrison, *supra* note 141.

235. Lilian Ablon et al., *Consumer Attitudes Toward Data Breach Notification and Loss of Personal Information*, RAND CORP. (2016), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf [perma.cc/Z2CH-4YVT].

236. *See id.* at x–xiii.

237. *See id.* at 16.

238. *See id.* at 17.

239. *See id.* at 29.

240. *See id.* at 19 (covering mostly financial and health information, such as credit card numbers, social security numbers, user account information, and more. Data about personality traits, habits, activities, and otherwise nonpersonal information is not covered in the study and remains outside of the traditional scope of data-breach law, which may pose a harm to consumers in the future).

Empirical research also supports the assertion that current data-breach notification laws reduce the likelihood of identity theft.[241] Consumers can act in a more informed fashion to restore their rights and protect their interests once the information gap is reduced. But there is certainly room for improvement—for example, by incentivizing and educating consumers on their rights and possible courses of action in the aftermath of a data breach.

Overall, the mere knowledge that manipulation could take place as a result of data-breach is invaluable for individuals whose data has been compromised. It may not be enough to inform consumers that their personal information was compromised, but also that such information is likely to be used for manipulation. The reduction of information gaps such as those addressed by data breach notification should be an indispensable part of the struggle to contain the effects of online manipulation.

B. INDIRECT REGULATION OF DATA COLLECTION

Data-breach notification law, if applied to manipulation, could inhibit the collection of every single data point that online actors collect about their respective consumers.[242] Storage costs are ever decreasing, meaning that data collectors often collect data before having a concrete use for it:[243] a phenomenon described "data warehousing."[244] This makes economic sense from the perspective of the collector; however, it creates an insurmountable harm to privacy, security, and autonomy, as it becomes a precious data trove for malicious actors to exploit.[245] Increasing the cost on data warehousing is likely to decrease the phenomenon, as hoarding companies would not gain as much benefit from it.

---

241. Romanosky et al., *supra* note 62, at 268.

242. *See* NAT'L PUB. SAFETY P'SHIP, FAIR INFORMATION PRACTICE PRINCIPLES (FIPPS) IN THE INFORMATION SHARING ENVIRONMENT (ISE) 2 (1974), https://www.nationalpublicsafetypartnership.org/Documents/The_Fair_Information_Practice_Principles_in_the_Information_Sharing_Environment.pdf [perma.cc/PU5W-7YLQ] ("PII should be collected only if the data is directly relevant and necessary to accomplish the specified purpose.").

243. *See* McClurg, *supra* note 37, at 73 ("Plummeting data storage costs make it economical for corporations to warehouse data for which they have not yet determined a use.").

244. *See* Joel Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1323 (2000) ("[D]ata warehousing is the stockpiling of millions of bits of personal information for future analysis.").

245. *See* Shaun B. Spencer, *The Problem of Online Manipulation*, U. ILL. L. REV. (forthcoming 2020) (manuscript at 61–62) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3341653 [https://perma.cc/SLN8-M6WE] (providing an example of a solution to online manipulation focused on, among other things, the collection of data—"if no data can be collected, then there would be no data to build the dossiers used to target and manipulate consumers. Constraining collection, however, would prohibit marketers from many other uses of that data, such as analyzing the practices and preferences of their own consumers").

This danger persists even in cases of the so-called "anonymized databases," which remove personal identification, because they have been proven to be "deanonymizable."[246] Paul Ohm advocates limiting data collection as a solution to the ability to reidentify anonymized databases, particularly when information privacy and security law does not recognize such "anonymized" data as protected under the law.[247] He suggests that regulators rein in privacy harms "by squeezing and reducing the flow of information in society, even though in doing so they may result in the need to sacrifice . . . values like innovation, free speech, and security."[248] There are many ways in which regulators could do so, some more contentious than others, but certainly covering a broad scope of data under data-breach notification laws would end up limiting what data is being collected by the covered entities.

The best practices of privacy protection, based on the Privacy Act of 1974, have come to be known as the Fair Information Practice Principles (FIPPs). These include "data minimization" as a key principle.[249] Minimization means that collection should only take place where "PII . . . is directly relevant and necessary to accomplish the specified purpose(s)" and should only be retained "for as long as is necessary to fulfill the specified purpose(s)."[250] While this principle is recognized, it is not legally binding. The way to enhance compliance with that principle is to increase the cost on entities that do not minimize. Therefore, data-breach notification law which covers a broad scope of data would increase the risks and costs on entities that collect information beyond what is required for their operation, as such extraneous information would expose them to legal liability.

The risk of collecting seemingly irrelevant data is also exemplified in the concept of sensor fusion.[251] Sensor fusion means that sensor data from different devices, combined together, would increase the capacity of making inferences about the user of these devices.[252] Scott Peppet explains that "data

246. *See* Ohm, *supra* note 158, at 1703.

247. *Id.* at 1766.

248. *Id.* at 1706.

249. *See* HUGO TEUFEL III, DEP'T OF HOMELAND SEC., PRIVACY POLICY GUIDANCE MEMORANDUM NO. 2008-01 4 (Dec. 29, 2008) https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf [perma.cc/CWF9-EA5Y] ("DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).").

250. *Id.*

251. *See* Scott Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 93 (2014) (" '[S]ensor fusion' dictates that the information from two disconnected sensing devices can, when combined, create greater information than that of either device in isolation.").

252. *See* Article 29 Data Protection Working Party, 8/2014 Opinion on the Recent Developments on the Internet of Things, (Sept. 16, 2014) at 7 n.6, https://ec.europa.eu/

gleaned from various small sensors can be combined to draw much more complex inferences than one might expect" and that data on simple movements, heart-rate, and even the way an individual holds her cellphone can tell us a lot about that person's mental and emotional state.[253] The sensor fusion problem connects directly to the problem of manipulation using various data points. It is but one phenomenon that makes nonpersonal information useful for a variety of inferences, whether for psychographic profiling or for discrimination.[254] Nonetheless, such data is extremely valuable to malicious actors.

Clearly, curtailing data collection by online actors is not a panacea, as data is one of the fuels of innovation. It allows companies to enhance their products, prevent fraud, and provide more tailored services to their customers.[255] However, the indirect nature of the impact provided by data-breach notification laws does not directly limit what companies can collect and store, but rather what counts as protected information under the law. Thus, it only increases the likelihood that covered entities will take this factor into account when assessing risks associated with data breaches.[256] The broader the scope of personal information, the more likely it is that companies will invest significant resources in securing that information, or perhaps even avoid collecting such data points altogether, as the risk may not be worth the potential benefit.

---

justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf [perma.cc/3K4P-PK7K] ("Sensor fusion consists in combining sensor data or data derived from different sources in order to get better and more precise information than would be possible when these sources are working in isolation."); *see also* Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats of Privacy and Security*, 31 BERKELEY TECH. L.J. 997, 1005–06 (2016) ("IoT [Internet of Things] is intimately connected to the notion of big data: collecting and storing a large amount and variety of granular data in real time, and using data analytics to reveal insights from these data. Putting together all the data from the device layer in a big data 'lake' enables its analysis in the context of other information, helping previously unseen linkages, patterns, and inferences emerge."); Peppet, *supra* note 251, at 115 ("More personal, perhaps, researchers are beginning to show that existing smartphone sensors can be used to infer a user's mood; stress levels; personality type; bipolar disorder; demographics (e.g., gender, marital status, job status, age); smoking habits; overall well-being; progression of Parkinson's disease; sleep patterns; happiness; levels of exercise; and types of physical activity or movement.").

253. *See* Peppet, *supra* note 251, at 121.

254. *Id.* at 117.

255. Calo, *supra* note 22, at 1042–43.

256. Solove & Citron, *supra* 39, at 745 ("[T]he very companies being sued for data breaches make high-stakes decisions about cyber security based upon an analysis of risk.").

C. REMEDYING VICTIMS OF MANIPULATION

Recognizing manipulation based on a data breach as harm would empower plaintiffs to sue in courts to remedy their harm, if such harm indeed materializes beyond mere risk. It would make manipulation a legally cognizable harm, which is a "harm that the law recognizes as worthy of redress, deterrence, or punishment."[257] As the Supreme Court recognized in *Spokeo v. Robins*, such harm could be either tangible or intangible.[258] It would effectively create a framework of legally cognizable manipulation, making data breaches costlier for companies. Currently, these data-breach litigation hurdles on plaintiffs do not impose the full potential of costs on the private corporations who have been breached.[259]

This redress would not only empower breach victims, but also increase overall information security. While the costs of disclosure (disclosure tax) is considered a deadweight loss, a consumer redress would transfer costs between consumers and breached entities, creating an actual incentive for these entities to reduce the externalities caused by data breaches, thus minimizing social cost.[260] This would increase information security, minimize harmful data collection practices, and remedy victims in the cases where breach and manipulation would still take place.

D. REGULATORY OVERSIGHT

Section 45 of the Federal Trade Commission Act already empowers the FTC to investigate and pursue legal action against companies who engage in "unfair or deceptive acts or practices in or affecting commerce."[261] As the Third Circuit held in *FTC* v. *Wyndham Worldwide Corp.*, the FTC has an

257. *Id.* at 747.

258. *See* Spokeo v. Robins, 136 S. Ct. 1540, 1549 (2016) ("Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete.").

259. *See* Tal Zarsky, *Data-Breach Harms—Bringing in the Courts, or Leaving them out?*, JOTWELL (Feb. 19, 2019), https://cyber.jotwell.com/data-breach-harms-bringing-in-the-courts-or-leaving-them-out/ [perma.cc/J6YP-FK5M].

260. *See* Sasha Romanosky et al., *Data Breaches and Identity Theft: When is Mandatory Disclosure Optimal?*, *in* WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY 26 (2010) ("We find that both disclosure tax and consumer redress cause the firm to increase its level of care, but only the disclosure tax represents deadweight loss, while redress represents a transfer of costs between the consumer and firm. Therefore, only an increase in redress can reduce the externality caused by the data breach. Further, social cost is always decreasing in consumer redress, but if this is small enough, some disclosure tax is necessary to reduce social cost. Therefore, if the firm bears only a small portion of consumer harm, the social planner may be justified in applying (or threatening to apply) additional fines or fees on the firm in order to minimize social cost.").

261. 15 U.S.C. § 45(a)(1) (2018).

authority under the "unfair" prong to regulate data security.[262] This is now largely the source of authority for the FTC to enforce data security laws against companies whose practices are inadequate and result in harm to consumers. This authority also does not contravene the state data-breach notification law framework. Indeed, the U.S. District Court for the District of New Jersey in *Wyndham* explicitly acknowledged that the FTC regulatory authority over data security may "coexist with the existing data security regulatory scheme."[263] Therefore, on the federal level, the FTC may pursue action against companies whose data security practices are deemed "unfair."

It is yet to be seen whether the FTC will also confront manipulation, both directly by online service providers and by third parties who obtain access to data through breaches. In particular, the FTC's ability to enforce cybersecurity practices leading to data breach harms other than identity theft or financial fraud may be constrained. Recently, the Eleventh Circuit in *LabMD v. FTC* held that the FTC needs to be very specific about what it means by "unfair or deceptive" with regard to data security.[264] However, this may be an opportunity for the FTC to clarify what harms and threats ought to be protected by cybersecurity law, and perhaps include manipulation within this ambit.

The FTC is, in a sense, a gap-filler because the data-breach law framework pertains, for the most part, to state legislation which focuses on exceptional incidents—data breaches. The FTC is relevant when manipulation is carried out by the primary data collector. An indication of the FTC's willingness to engage in such enforcement may be strengthened by its institution of a non-public investigation against Facebook in the Cambridge Analytica aftermath.[265] In addition, former FTC Commissioner Terrell McSweeny suggested that "the Commission should continue to study the effect of . . . custom audience tools and psychographics . . . to better scope their potential risks and to inform its enforcement."[266] Reevaluating the meaning of data breach in the context of

262. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015) (affirming the district court's decision that the FTC has authority).

263. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 613 (D.N.J. 2014).

264. LabMD, Inc. v. FTC, 894 F.3d 1221, 1236 (11th Cir. 2018) ("In sum, the prohibitions contained in cease and desist orders and injunctions must be specific. Otherwise, they may be unenforceable. Both coercive orders are also governed by the same standard of specificity, as the stakes involved for a violation are the same—severe penalties or sanctions.").

265. Press Release, Fed. Trade Comm'n, Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices (Mar. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection [perma.cc/99J3-TQQE].

266. *See* McSweeny, *supra* note 27, at 528 ("Considerations for the agency include whether advanced targeting technologies and tools that are neutral on their face are, in fact, having disparate impacts in violation of civil rights and equal opportunity laws and whether some of the tools are so manipulative that disclosures are ineffective. For example, not much is known

manipulation would better inform the FTC's enforcement practices, as these often derive their authority from existing statutes that reflect the same outdated notions of breach, harm, and personal information.[267]

But the key point about data-breach notification law in the context of regulatory oversight is that more clarity on how it relates to manipulation could also empower state attorneys general in investigating breaches that could result in manipulation of their respective states' residents. In the immediate aftermath of the Cambridge Analytica scandal, a bipartisan group of forty-one state attorneys general opened an inquiry against Facebook, demanding answers on how their respective residents' data was misused.[268] A more coherent approach on the relationship between data breach and manipulation could improve enforcement on the state side.

E. MANIPULATION AND THE FIRST AMENDMENT

Typically, when theoretical and doctrinal research revolves around the regulation of manipulation, or any other use or collection of information by corporations, a difficulty in terms of the First Amendment arises. Some argue that regulating manipulation would be a restriction on free speech, meaning that such regulation could not be possible without being unconstitutional.[269] Under this construction, the manipulator has her own speech interests, and the government will need a compelling argument to justify restriction of such manipulative speech.[270]

The Supreme Court has previously struck down a law passed by Vermont that sought to "restrict the sale, disclosure, and use of pharmacy records that

about whether and how psychographic targeting powered by massive amounts of data and automated technology works. It has variously been described as both 'powerful enough to influence elections' and 'an imprecise science at best and snake oil at worst.' ").

267. FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE 1 (2017), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf [perma.cc/T92P-XXMK] ("The FTC also has authority to enforce a variety of sector specific laws, including the Truth in Lending Act, the CAN-SPAM Act, the Children's Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act.").

268. Press Release, John Shapiro, Pa. Attorney Gen., Attorney General Shapiro Leads Bipartisan Coalition of State AGs in Demanding Answers from Facebook (Mar. 26, 2018), https://www.attorneygeneral.gov/taking-action/press-releases/attorney-general-shapiro-leads-bipartisan-coalition-of-state-ags-in-demanding-answers-from-facebook [perma.cc/8WSH-VXEZ].

269. *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1051 (2000).

270. *See* Sunstein, *supra* note 24, at 238.

reveal the prescribing practices of individual doctors."[271] The Court reasoned that content-based regulation cannot be justified solely on the grounds of "fear that people would make bad decisions if given truthful information," and therefore, "the State may not seek to remove a popular but disfavored product from the marketplace by prohibiting truthful, nonmisleading advertisements that contain impressive endorsements or catchy jingles. That the State finds expression too persuasive does not permit it to quiet the speech or to burden its messengers."[272]

This is an important hurdle to keep in mind while considering how to tackle online manipulation. However, the arguments advanced by this Article sidestep the First Amendment concern. Primarily, the solution proposed by this Article does not directly restrict speech in the form of the collection or use of information. Rather, it imposes mandatory disclosure of data breaches that are likely to result in manipulation.

Manipulators may claim that their activities are protected by the First Amendment. However, there is a substantial body of law constraining deception.[273] In addition, regulation of false or deceptive commercial speech is permissible in certain circumstances.[274] This legitimate regulation may also be appropriate for online manipulation, particularly if we accept that such manipulation often includes deceiving and lying.[275]

Scholars realize that influencing data subjects is fundamentally different than convincing them, and that the First Amendment doctrine to date cannot withstand the ever-increasing manipulation online.[276] The work of Micah Berman suggests that "it will become harder and harder for the courts to ignore the growing disconnect between doctrine and reality . . . the increased use—or misuse—of neuromarketing and sensory marketing research to influence consumers at a nonconscious level is likely to prompt calls for regulation."[277]

---

271. *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 557 (2011).

272. *See id.* at 577–78.

273. Gregory Klass, *The Law of Deception: A Research Agenda*, 89 U. OF COLO. L. REV. 101, 105 (2018) (defining deception as "an act or omission that wrongfully causes a false belief in another. The law of deception comprises laws designed to prevent, punish, compensate for, or otherwise address deception").

274. *Id.* at 235 (citing Va. State Pharmacy Bd. v. Va. Citizens Consumer Council, 425 U.S. 748 (1976) as an example of regulation of false or misleading speech).

275. *Id.* at 215 ("[T]here is a great deal of work on lies and deception and we can identify an overlap among lying, deceiving, and manipulating.").

276. Micah Berman, *Manipulative Marketing and the First Amendment*, 103 GEO. L.J. 497, 543 (2015) (suggesting that the government can find an interest in excluding manipulation from First Amendment's protection, such interest could be (but not limited to): "protecting public health (or other substantial state interests, such as public safety or environmental protection) by preventing consumers from being manipulated into harmful actions").

277. *Id.* at 546.

This indicates that a shift in First Amendment doctrine is anticipated in the wake of ubiquitous manipulative behavior online. Indeed, the First Amendment provides less protection on the *collection* and *use* of information, as opposed to *sale* and *disclosure*.[278] Since manipulation is achieved for the most part through collection and use, it is likely that the First Amendment will not invalidate the regulation of these practices.[279]

V. CONCLUSION

Online manipulation for political purposes is a dangerous emerging phenomenon which requires the utmost attention of cybersecurity law. The victims of such manipulation are often unaware of its existence, details, and sophistication. As this Article has argued, data-breach notification law is one example of an area where cybersecurity law may be effective in addressing harmful online manipulation by imposing a duty on breached entities to inform potential victims, though by no means this is the only solution to respond to emerging cybersecurity threats. This requires a reevaluation of what cybersecurity law seeks to protect, in light of the emerging threats enabled by new uses of personal data using new tools such as psychographic profiling through machine learning.

Recent indications from federal and state authorities point to an inclination to reconsider cybersecurity law and its applicability to online manipulation. As this Article has outlined, there is much to consider in that context. Immediate legal intervention is desperately needed to enhance our collective privacy, autonomy, and democracy in the information age. However, existing bodies of cybersecurity law, such as data-breach notification law, can achieve this goal until a more comprehensive and direct regulatory approach is ultimately adopted.

278. Balkin, *supra* note 28, at 1194.

279. Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1182 (2005).