ARTICLE

DATA SCAMS

Roger Allan Ford[*]

ABSTRACT

Targeting platforms like Google and Facebook are usually seen as presenting tradeoffs between utility and privacy. This Article identifies and describes a different, non-privacy cost of targeting platforms: they make it easier for malicious actors to scam others. They do this by making it easier for scammers to reach the most promising victims, hide from law-enforcement authorities and others, and develop better scams. Technology offers potential solutions, since the same data and targeting tools that enable scams could help detect and prevent them, though neither platforms nor law-enforcement officials have both the incentives and expertise needed to develop and deploy those solutions. Moreover, these scams may illustrate a broader class of

* Professor of Law, University of New Hampshire Franklin Pierce School of Law; Faculty Fellow, Franklin Pierce Center for Intellectual Property; Affiliated Fellow, Information Society Project, Yale Law School. For helpful comments and conversations, I am indebted to Aaron Burstein, Adam Bonin, Alex Roberts, Amy Vorenberg, Andrew Selbst, Ann Bartow, Bill Murphy, Bonnie Kaplan, Cathay Smith, Chris Hoofnagle, Craig Wills, David Hyman, Dmitry Karshtedt, Emily McReynolds, Emily Michiko Morris, Erik Hovenkamp, Jack Balkin, Jake Linford, Jennifer Berk, Jennifer King, Jessica Kiser, Jim Lindgren, John Greabe, John Orcutt, Joris van Hoboken, Julie Cohen, Kate Klonick, Laura Moy, Lauren Willis, Lisa Bernstein, Marcus Hurn, Paul Ohm, Peter Guffin, Rebecca Crootof, Ryan Calo, Ryan Vacca, Sarah Schindler, Siona Listokin, Terrell McSweeny, Tom Hemstock, Tonya Evans, Victoria Schwartz, Whitney Merrill, Zahr Said, and Zvi Rosen, and to the organizers and participants at the tenth Privacy Law Scholars Conference, the fifth Junior Intellectual Property Scholars Association workshop, the Information Society Project's Ideas Lunch, faculty workshops at the University of New Hampshire, University of Maine, and Benjamin N. Cardozo School of Law, and Legal Scholarship Workshops at the University of Chicago and Northwestern University.

problems from targeting that go beyond utility versus privacy, suggesting that more aggressive interventions may be needed.

TABLE OF CONTENTS

I. INTRODUCTION

In the course of the historically strange 2016 presidential election, one of the stranger subplots came in the form of a political action committee called the American Horizons PAC, which purported to support Donald Trump.[1] The PAC, created by

1. Shane Goldmacher, *Meet the Man Siphoning Money from Donald Trump*, POLITICO (Aug. 29, 2016, 5:25 AM), http://politico.com/story/2016/08/donald-trump-fundraiser-hawes-227486 [https://perma.cc/AY48-KM2J].

twenty-five-year-old Ian Hawes, raised more than $1.1 million in 2016 by offering donors the chance to win a "Dinner with Donald Trump" if they signed up at dinnerwithtrump.org. As the fine print explained, this meant that the PAC would buy the winner two tickets to a Trump fundraiser. The PAC could offer little more: though its website looked eerily like the Trump campaign's, and though many donors thought they were giving to the campaign, the two groups were entirely unaffiliated. Of the $1.1 million the group raised, it spent only $31,000 supporting the Trump campaign—and even that much might be doubted, since much of the money was spent through a company owned by Hawes.[2]

Scam PACs and other organizations have been around for a long time; a certain kind of low-end political organization has long used direct mail to raise money, much of which is used, in turn, for further fundraising.[3] But American Horizons represented an innovative escalation of these efforts. Instead of painstakingly building a donor list or purchasing an expensive premade list from a broker, American Horizons bought Facebook ads—$108,000 of them in just three weeks.[4] Because Facebook had already done the work to identify likely Trump supporters and made that conclusion available to advertisers through its platform, American

2. American Horizons' FEC filings report that $26,000 out of $31,000 in Trump-supporting independent expenditures were made with CartSoft, LLC. AMERICAN HORIZONS PAC, FEC FORM 3X: REPORT OF RECEIPTS AND DISBURSEMENTS 1–4, 33 (Oct. 26, 2016) [hereinafter AMERICAN HORIZONS PAC, OCTOBER FEC FORM 3X], https://docquery.fec.gov/pdf/999/201610269034584999/201610269034584999.pdf [https://perma.cc/KM5L-QH3S]; AMERICAN HORIZONS PAC, FEC FORM 3X: REPORT OF RECEIPTS AND DISBURSEMENTS 1–4, 37–38 (Dec. 8, 2016) [hereinafter AMERICAN HORIZONS PAC, DECEMBER FEC FORM 3X], https://docquery.fec.gov/pdf/975/201612089039945975/201612089039945975.pdf [https://perma.cc/3YUP-6FX8]. Politico reports that Hawes owns CartSoft. Goldmacher, *supra* note 1. On top of the $26,000 spent supporting Trump's campaign, the PAC's filings also report more than $392,000 in operating expenses spent with CartSoft, for "payment software development" and "campaign strategy consulting." AMERICAN HORIZONS PAC, OCTOBER FEC FORM 3X, *supra*, at 168.

3. *E.g.*, Kenneth P. Vogel, *The Rise of 'Scam PACs*,*'* POLITICO (Jan. 26, 2015, 5:35 AM), http://www.politico.com/story/2015/01/super-pac-scams-114581 [https://perma.cc/EU69-Y7FK] ("Since the tea party burst onto the political landscape in 2009, the conservative movement has been plagued by an explosion of PACs that critics say exist mostly to pad the pockets of the consultants who run them. . . . [T]he PACs plow most of their cash back into payments to consulting firms for additional fundraising efforts."); *see also* RICK WILSON, EVERYTHING TRUMP TOUCHES DIES 4–5 (2018) ("If I'd been truly amoral, I could have easily spun up a ScamPAC called Americans Making America Great Again American Eagle Patriot Trump Brigade for Freedom Build the Wall Anti-Sharia PAC. AMAGAAEPTBFFBTWAS PAC would have dropped a few million fundraising emails to the obviously enormous ocean of credulous boobs who click 'Donate' at the sign of a red hat and a sparkly eagle gif, and watched the donations roll in. I could have my volcano lair by now.").

4. Goldmacher, *supra* note 1.

Horizons could quickly and efficiently show its ads to many of the most promising potential contributors.

In one sense, this use of targeting is nothing new. Advertisers have always looked for ways to find the most promising audiences for their ads, whether by advertising in venues favored by preferred demographics or by sending targeted direct mail or e-mail to consumers thought to be likely customers.[5] New data tools and techniques make this process more efficient and might allow advertisers to find new ways to target and manipulate customers,[6] but the goal of advertising goods and services to consumers remains the same. The ends, though, are different: just as data makes it easier, cheaper, and more efficient to sell goods and services, it makes it easier, cheaper, and more efficient to defraud consumers, sell worthless products, and commit all kinds of low- and high-level scams.[7]

This Article considers the implications of modern data tools and techniques—widespread use of data analytics, datasets of consumer information, and online targeting platforms—for scams like the American Horizons PAC. Traditional advertising can be socially valuable when it educates and informs consumers and helps match them with useful goods and services.[8] Much of the

5. *See infra* Section II.B.

6. *See, e.g.*, SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 282–90 (2019); Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1003–18 (2014); Daniel Susser et al., Online Manipulation: Hidden Influences in a Digital World 24–29 (Dec. 23, 2018) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3306006 [https://perma.cc/7Q6H-V7NU].

7. I use "scams" in a broad sense not dictated by the law, though many scams will be illegal. *See infra* Section III.A (developing a definition of "scam" in which a perpetrator takes advantage of a victim, regardless of the legality of the scam). American Horizons, for instance, may not have done anything illegal; the fine print on its website explained exactly what it was offering, and it appears to have complied with the FEC's reporting requirements for political action committees. It also refunded many contributions upon requests from donors. The Trump campaign, for what it's worth, accused American Horizons of fraud, but doesn't seem to have done anything more than send a cease-and-desist letter and file a statement with the FEC explaining that the two entities are unrelated. *See* Shane Goldmacher, *Trump Campaign Demands 'Dinner with Trump' Super PAC Cease and Desist*, POLITICO (Aug. 29, 2016, 6:40 PM), https://www.politico.com/story/2016/08/trump-campaign-super-pac-dinner-227520 [https://perma.cc/WFT2-FBD8]; DONALD J. TRUMP FOR PRESIDENT, INC., FEC FORM 99 (Aug. 29, 2016), https://docquery.fec.gov/pdf/861/201608299023756861/201608299023756861.pdf [https://perma.cc/3VJ9-VDJQ]. But American Horizons' strategy appears to be designed primarily to benefit Hawes and his companies rather than the Trump campaign, since many of Horizons' expenses were routed through those companies and little of its spending even purported to benefit the Trump campaign. American Horizons did this by falsely convincing at least some contributors that they were directly helping the Trump campaign, not an unrelated PAC. *See* Goldmacher, *supra* note 1 (reporting that out of eleven contributors that Politico was able to reach, all believed they were giving to the Trump campaign).

8. *See infra* Section II.A.

literature on targeted advertising considers the tradeoffs between efficiency gains from better consumer targeting and the privacy costs of that targeting.[9] With scams, though, there is no argument for socially valuable targeting, since the goods and services being marketed are themselves socially harmful.[10] Yet targeting platforms facilitate these scams by making three things easier and cheaper: finding the most promising victims, avoiding detection by law-enforcement agencies and others, and developing the most effective and persuasive scams. When targeting platforms facilitate scams, there is no privacy-efficiency tradeoff; instead, the better the targeting, the worse it is for society.[11]

There are interventions that could help solve these problems, but they are difficult to implement and would bring their own problems. A naïve solution would be to ban targeted advertising, but such a rule is politically unviable and would impose significant costs. A better approach might be to use the same datasets and analytics tools that enable targeting to help expose scams by revealing patterns characteristic of scammers.[12] The critical question is how the government could encourage the development of tools to reveal these patterns. Platforms could give law-enforcement agencies access to the necessary data, but agencies may not be competent to use the data, and giving them this access would create new privacy problems.[13] Platform developers could instead do some of the work themselves, since they likely have the needed expertise in their own platforms and in analyzing complex data. Platforms lack strong incentives to detect scams, though, because scams can increase platform profits and since federal law makes it difficult to compel platforms to help.[14] Giving platforms incentives to detect scams, then, while providing officials access to enough data to enforce the law while not compromising users' privacy, requires a careful regulatory balance.

This analysis has important implications for policy makers and scholars of privacy and targeting technologies. Data scams have their roots in aggregated personal information, but their harms are not obviously privacy harms, since they don't stem from the disclosure of personal information. And they're not alone in this anomaly. Targeting platforms create several kinds of non-

9. *See infra* Section II.B.
10. *See infra* Section III.A.
11. *See infra* Section III.B.
12. *See infra* Section IV.A.
13. *See infra* Section IV.B.
14. *See infra* Section IV.C.

privacy harms in the consumer marketplace and the democratic system. Yet platforms do not often bear the costs of these harms, suggesting a need for regulation. Moreover, if the benefits of targeting are smaller than they seem—a plausible conclusion from the limited available evidence—then perhaps the naïve solution of an outright ban on targeting has something to recommend it.[15]

The rest of this Article proceeds as follows. Part II provides background, briefly reviewing the economic debate on the social value of advertising and the literature on privacy and targeted advertising. Part III extends this literature into the realm of scams and other forms of socially harmful targeting, arguing that the targeting techniques discussed in Part II make it easier for scammers to target victims and harder for law-enforcement agencies to detect and prevent these scams. Part IV discusses ways that technology could be used to address the problem of data scams, how law-enforcement agencies and platforms could be encouraged to develop those technologies, and difficulties in implementing each approach. Part V discusses implications.

II. TARGETED ADVERTISING

Perpetuators of data scams use the same forms of targeted advertising that legitimate sellers use to market their goods and services. This Part provides a brief overview of these targeted advertising tools, first discussing advertising more generally and then discussing how data analytics, consumer datasets, and targeting platforms permit more efficient advertising. Because advertising by legitimate firms is well entrenched and, arguably, welfare-enhancing, the solution to data scams is unlikely to be simply to eliminate these forms of advertising.[16]

A. The Social Value of Advertising

For a ubiquitous feature of modern life, advertising presents some surprisingly difficult economic puzzles. In a world of perfect competition, advertising would be pure waste, but firms nevertheless spend half a trillion dollars a year advertising their products.[17] Economists have long asked, then, what effects

15. *See infra* Part V.

16. *But see infra* Part V.

17. *E.g.*, *Global Ad Spending Growth to Double This Year*, EMARKETER (July 9, 2014), https://www.emarketer.com/Article/Global-Ad-Spending-Growth-Double-This-Year/1010997 [https://perma.cc/MZ6L-44SS] (reporting that advertisers were expected to spend $545.40 billion worldwide on advertising in 2014).

advertising has on consumers and whether those effects are socially valuable.[18]

In general, three theories have been proposed about how advertising affects consumers.[19] The first theory asserts that advertising persuades consumers, such as by altering their demand for an advertiser's products or creating loyalty to the advertised brands.[20] The second theory asserts that advertising informs consumers by providing information that reduces consumers' search costs. This can be information about the product (such as pricing or specifications) or indirect information that signals something about the advertiser or product (such as that the company has money to spend on advertising).[21] And the third theory asserts that advertising complements the advertised

18. See generally Kyle Bagwell, *The Economic Analysis of Advertising*, *in* 3 HANDBOOK OF INDUSTRIAL ORGANIZATION 1701 (Mark Armstrong & Robert H. Porter eds., 2007); John Philip Jones, *The Economic Effects of Advertising: How Research Can Untangle Them*, *in* THE HANDBOOK OF INTERNATIONAL ADVERTISING RESEARCH 51 (Hong Cheng ed., 2014), for useful overviews of the economic literature on advertising.

19. *See* Bagwell, *supra* note 18, at 1708–24.

20. *See id.* at 1710–16. Some of the key works in the development of the persuasion theory include WILLIAM S. COMANOR & THOMAS A. WILSON, ADVERTISING AND MARKET POWER 41–63 (1974) (reviewing theory and evidence suggesting that advertising can be a significant source of barriers to entry in consumer-product industries due to brand loyalty and other factors consistent with the persuasion theory); JOHN KENNETH GALBRAITH, THE AFFLUENT SOCIETY 155–56 (1958) (arguing that advertising and sales create demand for products and that "the manufacturing of demand for the product" is as important, or more important, to businesses as the manufacturing of the product itself); VANCE PACKARD, THE HIDDEN PERSUADERS 3–5 (1957) (arguing that advertisers prey on consumers' psychological vulnerabilities to create new desires and persuade them to buy goods); Dorothea Braithwaite, *The Economic Effects of Advertisement*, 38 ECON. J. 16, 17–23 (1928) (considering advertising as a "selling cost" that shifts consumer demand but might also provide economies of scale that reduce prices for consumers); Nicholas Kaldor, *The Economic Aspects of Advertising*, 18 REV. ECON. STUD. 1, 4–5, 7, 13–15 (1950) (concluding that although advertising can inform or persuade, most is likely intended to persuade given the advertiser is an interested party and also developing the argument that advertising increases industry concentration due to scale economies).

21. *See* Bagwell, *supra* note 18, at 1716–20. Some of the key works in the informative theory include Phillip Nelson, *Advertising as Information*, 82 J. POL. ECON. 729 (1974) (exploring different ways that advertising can provide information about search goods and experience goods); S.A. Ozga, *Imperfect Markets Through Lack of Knowledge*, 74 Q.J. ECON. 29, 39–40 (1960) (proposing that diminishing returns from advertising arise because the more people that see an ad, the greater the fraction of people who have already received its information, and so the greater the fraction of subsequent advertising dollars that are wasted); George J. Stigler, *The Economics of Information*, 69 J. POL. ECON. 213, 223–24 (1961) (developing a model of consumer behavior in response to dispersed prices and arguing that advertising serves as a source of pricing information that reduces price dispersion, reducing retailer margins and benefiting consumers); Lester G. Telser, *Advertising and Competition*, 72 J. POL. ECON. 537, 541–51 (1964) (finding evidence that advertising can facilitate market entry by giving consumers information about new products).

goods or services, such as by creating a perception of luxury that consumers of an expensive product desire.[22]

There is likely some truth in each of these stories, but the problem is that they lead to inconsistent conclusions.[23] The optimistic case for advertising largely derives from the second theory, that advertising informs consumers and reduces their search costs.[24] Advertising provides several forms of information. The most direct form consists of facts about the advertised goods and services, like product features and pricing.[25] Such information is socially valuable because it helps consumers find better and cheaper products and because it forces companies to compete to produce and sell those products, reducing margins. Without this information, some consumers would pay higher prices, and others would buy products without features they would otherwise want, in both cases out of ignorance of better options. And without the ability to tell consumers about their products, new entrants to a market would have a hard time competing with established sellers. But advertising also provides several kinds of indirect information.[26] The simple fact that a firm advertises suggests a degree of corporate health, suggesting that the firm is likely to be

22. *See* Bagwell, *supra* note 18, at 1720–23. Some of the key works in the complementary theory include Gary S. Becker & Kevin M. Murphy, *A Simple Theory of Advertising as a Good or Bad*, 108 Q.J. ECON. 941 (1993) (analyzing the consumer-welfare effects of complementary advertising and demonstrating that, in some circumstances, advertising may be undersupplied); Len M. Nichols, *Advertising and Economic Welfare*, 75 AM. ECON. REV. 213, 213–15 (1985) (analyzing the same); George J. Stigler & Gary S. Becker, *De Gustibus Non Est Disputandum*, 67 AM. ECON. REV. 76, 83–87 (1977) (demonstrating that even in a world of stable consumer preferences and perfect competition, advertising can provide value that complements the value of the advertised good, changing equilibrium prices).

23. John Philip Jones, for instance, identifies seven ways advertising can affect consumer prices—lowering prices in four cases and raising them in three. *See* Jones, *supra* note 18, at 56–69.

24. Portions of the other theories also suggest advertising can be a social good. For instance, all kinds of advertising can promote economies of scale, which can—but need not necessarily—reduce the cost of products. *See* Braithwaite, *supra* note 20, at 17–20; Jones, *supra* note 18, at 63–67; *see also infra* notes 30–31 and accompanying text. Likewise, all kinds of advertising reduce the cost to consumers of television, newspapers, websites, and other forms of media. *See* Jones, *supra* note 18, at 68–69. The complementary view of advertising also suggests that even ads with no apparent information content can be socially valuable. *See infra* note 29 and accompanying text.

25. *See, e.g.*, Stigler, *supra* note 21, at 220–24 (discussing pricing information in advertising); Telser, *supra* note 21, at 550–51, 556–57 (assessing information about new products in advertising); *see also* Phillip Nelson, *Information and Consumer Behavior*, 78 J. POL. ECON. 311, 312–18, 323–25 (1970) (introducing the concepts of search goods and experience goods and demonstrating how advertising can usefully provide information about each category of goods).

26. *See* Bagwell, *supra* note 18, at 18–19, 19 n.13 (quoting Nelson, *supra* note 21, at 734 (summarizing three reasons indirect information is provided to consumers)).

a reliable and efficient supplier.[27] Advertising also helps match consumers with products that best fit their tastes and remind consumers of their past positive experiences with a company.[28]

Advertising could also be socially harmful. One way this could work is if advertising shaped consumer demand instead of informing it; then it could have a distorting effect, shifting demand away from consumers' "true" or ideal preferences.[29] A consumer who sees ads for a car might buy that car, then, instead of a different, cheaper car that she would value more or that would better serve her needs; a consumer who sees ads for cigarettes might become addicted to nicotine as a teenager. A second mechanism would be if advertising promoted industry concentration; in particular cases this could be good (if economies of scale led to lower prices) or bad (if firms innovated less or charged higher prices because of reduced competition).[30] Advertising might promote concentration by building customer loyalty, erecting new barriers to entry; or it might do so because of economies of scale in advertising. If incumbents have more money to spend and more experience crafting ads—think of the in-house expertise a company like Procter & Gamble has in advertising dish soap and laundry detergent, and how much ground a new entrant would have to make up—then the incumbents would get better results per advertising dollar. This could create a feedback loop that promotes industry concentration. Alternatively, of course, advertising could help entrants break into the market by telling consumers about their products.[31]

Economic theory, then, can tell optimistic and pessimistic stories about advertising. Probably both stories contain some truth; there are many kinds of advertising, for many kinds of products, directed at many kinds of consumers. The empirical literature provides support for both stories.[32] Notably, however, several studies provide support for the information theory of

27. *See id.* at 18; Nelson, *supra* note 21, at 732–34.

28. *See* Bagwell, *supra* note 18, at 19; Nelson, *supra* note 21, at 733–34.

29. *See* GALBRAITH, *supra* note 20, at 129; PACKARD, *supra* note 20, at 3–10. Note, however, the important caveat that if persuasive advertising has value to consumers apart from its information value—say, from increasing the consumer's level of prestige in others' eyes—then it can be socially valuable even without appearing to provide information. *See* Becker & Murphy, *supra* note 22, at 942–45; Nichols, *supra* note 22, at 213–14.

30. *E.g.*, Braithwaite, *supra* note 20, at 34–36; Kaldor, *supra* note 20, at 13–15. For a review of the empirical literature on advertising scale economies and concentration see Bagwell, *supra* note 18, at 30–32.

31. For a review of the empirical literature on advertising's effect in deterring or facilitating entry, see Bagwell, *supra* note 18, at 45–47.

32. *See* Jones, *supra* note 18, at 56–69.

advertising and its implication that advertising can promote competition. First, a set of studies finds that advertising has the greatest effect on consumers who have not made recent purchases in the advertised category; otherwise, prior experience and loyalty or inertia plays a much greater role in dictating consumer behavior.[33] This suggests both that advertising has its greatest effect on the consumers most in need of information and that it can do only so much to shape consumer demand. Second, another set of studies shows that advertising can be especially effective when it introduces new products or new features of an existing product, informing consumers about those new products or features.[34] Third, a set of studies shows that consumers respond to specific information content in advertising. When producers of fiber-containing cereals promoted claims that the cereals helped prevent cancer, for instance, sales of those cereals spiked out of proportion to the simple quantity of advertising.[35]

The most plausible conclusion, then, is likely that advertising is, in many cases, socially valuable because it informs consumers and promotes innovation and competition. At the same time, in other cases—maybe certain types of advertising like false advertising[36] or advertising to children,[37] or advertising in certain

33. *See, e.g.*, John Deighton et al., *The Effects of Advertising on Brand Switching and Repeat Purchasing*, 31 J. MARKETING RES. 28, 37, 41 (1994); Gerard J. Tellis, *Advertising Exposure, Loyalty, and Brand Purchase: A Two-Stage Model of Choice*, 25 J. MARKETING RES. 134, 139–43 (1988).

34. *See, e.g.*, Daniel A. Ackerberg, *Empirically Distinguishing Informative and Prestige Effects of Advertising*, 32 RAND J. ECON. 316, 332 (2001); Matthew Shum, *Does Advertising Overcome Brand Loyalty? Evidence from the Breakfast-Cereals Market*, 13 J. ECON. & MGMT. STRATEGY 241, 245, 261–64 (2004).

35. *See* Pauline M. Ippolito & Alan D. Mathios, *Information, Advertising and Health Choices: A Study of the Cereal Market*, 21 RAND J. ECON. 459, 461, 479 (1990).

36. False advertising is prohibited by the Lanham Act and by most states' laws. *See generally* 5 J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 27 (5th ed. 2018).

37. No statute comprehensively regulates advertising to children, but two play prominent regulatory roles. *See* Children's Television Act of 1990, Pub. L. No. 101-437, 104 Stat. 996 (codified as amended at 47 U.S.C. §§ 303a–303b, 394 (2012)) (empowering the Federal Communications Commission to regulate children's television programming and advertising during that programming); 47 C.F.R. §§ 73.670–73.673 (2018) (implementing the Children's Television Act by requiring broadcast stations to air three hours of educational programming a week and limiting the number of commercials that can run during those programs); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (limiting the tools available for online advertising to children); 16 C.F.R. pt. 312 (implementing the Act). Moreover, the Federal Trade Commission pays special attention to advertising that targets children under its general consumer-protection authority. *See, e.g.*, J. Howard Beales, III, *Advertising to Kids and the FTC: A Regulatory Retrospective That Advises the Present*, 12 GEO. MASON L. REV. 873 (2004); FED. TRADE COMM'N, A REVIEW OF FOOD MARKETING TO CHILDREN AND ADOLESCENTS: FOLLOW-UP REPORT (2012), https://www.ftc.gov/sites/default/files/documents/reports/review-food-ma

product categories like tobacco[38] or prescription drugs[39]—advertising might be more problematic. The law has responded accordingly: false advertising and deceptive and unfair trade practices are illegal, and advertising in certain industries is highly regulated, but firms are otherwise largely free to advertise as they see fit.[40]

B. Consumer Datasets, Data Analytics, and Targeting Platforms

Technology has revolutionized advertising by making it possible to target individual consumers to an unprecedented degree, amplifying its effects in ways that heighten this welfare analysis. When advertising is a social good, this amplification means that targeted advertising can be an even greater social good; when advertising is a social ill, targeted advertising is likely an even greater social ill. The reason is straightforward. Whatever social role advertising plays, it plays that role only when it works,

---

rketing-children-and-adolescents-follow-report/121221foodmarketingreport.pdf [https://perma.cc/LZ8J-A6ZG]; FED. TRADE COMM'N, MARKETING VIOLENT ENTERTAINMENT TO CHILDREN: A SIXTH FOLLOW-UP REVIEW OF INDUSTRY PRACTICES IN THE MOTION PICTURE, MUSIC RECORDING & ELECTRONIC GAME INDUSTRIES (2009), https://www.ftc.gov/sites/default/files/documents/reports/marketing-violent-entertainment-children-sixth-follow-review-industry-practices-motion-picture-music/p994511violententertainment.pdf [https://perma.cc/JYM8-WNW7]; DEBRA J. HOLT ET AL., FED. TRADE COMM'N, CHILDREN'S EXPOSURE TO TV ADVERTISING IN 1977 AND 2004: INFORMATION FOR THE OBESITY DEBATE (2007), https://www.ftc.gov/sites/default/files/documents/reports/childrens-exposure-television-advertising-1977-and-2004-information-obesity-debate-bureau-economics/cabecolor.pdf [https://perma.cc/JNF6-SYJR].

38. The Food & Drug Administration regulates tobacco products, including their advertising. *See* Family Smoking Prevention and Tobacco Control Act, Pub. L. No. 111-31, 123 Stat. 1776 (2009) (codified as amended in scattered sections of 21 U.S.C.); *see also* 21 C.F.R. pt. 1140 (restricting the distribution of free samples for tobacco products).

39. Most countries prohibit direct-to-consumer advertising of prescription drugs. The United States is (along with New Zealand) an outlier; prescription-drug advertising is permitted but is regulated by the Food & Drug Administration. *See* 21 U.S.C. § 352(n); 21 C.F.R. § 202.1; *see also* Medicines Act 1981, ss 56–62 (N.Z.) (regulating medical advertisements). Advertisements that discuss the benefits of a drug must also disclose major side effects and contraindications. 21 C.F.R. § 202.1(e)(1). The effects of direct-to-consumer prescription-drug advertising have been extensively studied. *See, e.g.*, Abby Alpert et al., *Prescription Drug Advertising and Drug Utilization: The Role of Medicare Part D* (Nat'l Bureau of Econ. Research, Working Paper No. 21714, 2015) (finding that increased drug advertising after the launch of Medicare Part D led to increased drug utilization among younger patients not eligible for Medicare Part D); Dhaval M. Dave, *Effects of Pharmaceutical Promotion: A Review and Assessment* (Nat'l Bureau of Econ. Research, Working Paper No. 18830, 2013) (literature review concluding that advertising significantly increases drug sales, principally by expanding the market for that drug rather than by taking business from a competitor).

40. The right balance between the optimistic and pessimistic stories may also change over time. *See, e.g.*, Ramsi A. Woodcock, *The Obsolescence of Advertising in the Information Age*, 127 YALE L.J. 2270, 2299–2307 (2018) (arguing that the ready availability of product information on the internet renders the information content of advertising superfluous).

and the better targeted it is, the better it works (with some caveats to be explored shortly). When a car company advertises a new luxury model, it might aim to persuade consumers to buy the new car or to inform them about its benefits or to create a perception that the car is luxurious and driven by successful consumers, but regardless, its goal is to sell more cars. Advertising that reaches groups of consumers who are likely to buy the car can do a better job of persuading or informing or creating a perception in likely buyers' peer groups; advertising that reaches other, less-interested consumers is a waste of money.

There are two basic ways advertisers can target customers. One is indirect, using the advertising venue—the specific television show or network, magazine or newspaper, website, billboard location, and so forth—as a proxy for the kinds of people the advertiser wants to target.[41] This is sometimes called contextual advertising. Rolex and BMW sponsor tennis and golf tournaments and advertise on their broadcasts because wealthy people tend to watch and play those sports;[42] defense contractors advertise in the Washington subway stops near the Pentagon and Capitol so they'll be seen by staffers making procurement decisions;[43] the consulting firm Accenture advertises in airports in part to boost the morale of its frequent-flyer employees.[44] Sometimes the targeted group is the type of consumer who would be interested in the product, as when diapers are advertised to new parents or Medicare prescription-drug plans to the elderly. Other times the purpose is subtler. For instance, some sellers will advertise the same product to different audiences in different ways, trying to tailor the message to the audience. Or, some sellers

41. *See, e.g.*, Ambarish Chandra, *Targeted Advertising: The Role of Subscriber Characteristics in Media Markets*, 57 J. INDUS. ECON. 58, 76, 82–83 (2009) (finding that newspapers in competitive markets have higher advertising prices than similar newspapers in noncompetitive markets, because they can segment the market and better target specific groups of readers).

42. *E.g.*, Malcolm Moore, *Sponsorship on the Rise as Golf Participation Rates Fall*, FIN. TIMES (Sept. 19, 2015), https://www.ft.com/content/b75928c0-410b-11e5-b98b-87c7270955cf (quoting the head of a sports agency: "[E]ven when there are ups and downs in the economy, golf is still the sport of business and that makes it alluring to sponsors").

43. *E.g.*, Gary Leff, *Boeing Pitches a Fit After Losing Out on $80 Billion Defense Contract*, VIEW FROM WING (Nov. 7, 2015), https://viewfromthewing.boardingarea.com/2015/11/07/boeing-pitches-a-fit-after-losing-out-on-80-billion-defense-contract/ [https://perma.cc/7QNZ-KTN5]; Anne Riley, *Defense Lobbying Goes Underground*, OPENSECRETS (June 27, 2007), https://www.opensecrets.org/news/2007/06/defense-lobbying-goes-undergro/ [https://perma.cc/X6P6-EP4F]; Stephanie Westbrook, *Occupied, D.C.*, THESE TIMES (May 28, 2010), http://inthesetimes.com/article/6009/occupied_d.c [https://perma.cc/PV6J-TEJK].

44. Mark Suster, *The Silent Benefits of PR*, BOTH SIDES TABLE (Oct. 25, 2014), https://bothsidesofthetable.com/the-silent-benefits-of-pr-29ae38417e03 [https://perma.cc/MG6C-ZCZW].

will target audiences for strategic reasons, as when Subaru targeted rural audiences in the 1970s because they were less likely to have seen *Consumer Reports'* scathing review of the first car the company sold in the United States.[45] Whatever the purpose, indirect targeting is as old as advertising itself. It is necessarily wasteful, though, since every time a potential buyer of high-end watches sees a Rolex ad, so do many others who have no interest.[46]

The other form of targeting is direct and individualized. When a company can tell which specific consumers are most likely to be receptive to the message and has a way to advertise only to those consumers, it can avoid the waste inherent in less-targeted forms of advertising. Many types of advertising can't be customized on this sort of individual basis—a magazine can't realistically print different ads in each subscriber's copy, for instance.[47] Historically these factors have made individualized targeting rare, mostly limited to direct mail.[48] Direct mail is less engaging than other forms of advertising like television, though, so individualized targeting has historically had limited use.[49]

Even when individual targeting is possible, the techniques used to identify individual consumers are not free. Some of them are straightforward, like when a company keeps a mailing list of customers who have purchased its products in the past; those people are good targets because they have already demonstrated a need and affinity for the firm's products. Or a list broker might

45. *See* Bob Sorokanich, *How Subaru Became the Unofficial Car of Vermont*, ROAD & TRACK (Mar. 23, 2018), https://www.roadandtrack.com/car-culture/classic-cars/a19563992/how-subaru-became-the-unofficial-car-of-vermont/ [https://perma.cc/L49N-5GEL] (explaining how Subaru targeted rural areas in Vermont, Minnesota, Washington, New Hampshire, and western Pennsylvania because consumers there were less likely to have seen Consumer Reports' conclusion that the Subaru 360 was "unacceptably hazardous").

46. *See* Randal C. Picker, *The Digital Video Recorder: Unbundling Advertising and Content*, 71 U. CHI. L. REV. 205, 207 (2004).

47. Or at least, magazines haven't historically been able to do so, since offset printing has substantial fixed costs for each print run. But technology is making it possible. *See, e.g.*, D. Eadward Tree, *6 Ways to Grow Revenue with Digitally-Printed Magazines*, PUB. EXECUTIVE (Nov. 14, 2017), http://www.pubexec.com/post/6-ways-magazine-publishers-can-increase-revenue-digital-printing/ [https://perma.cc/4AS6-VA5P] (noting that when the magazine Farm Journal included a targeted 8-page advertising insert for just 450 subscribers, selected based on their purchasing history, it generated $50,000 in incremental revenue).

48. *See, e.g.*, DAVID OGILVY, OGILVY ON ADVERTISING 143–49 (1983); BOB STONE & RON JACOBS, SUCCESSFUL DIRECT MARKETING METHODS 287–88 (7th ed. 2001). Modern data brokers have gotten into the business as well. *See, e.g.*, *Direct Mail Marketing*, EXPERIAN, https://www.experian.com/small-business/direct-mail-marketing.jsp [https://perma.cc/8VJK-YGV8] (last visited Sept. 12, 2019).

49. *See generally* OGILVY, *supra* note 48, at 143; STONE & JACOBS, *supra* note 48, at 195, 287.

assemble a list of people who have purchased a certain kind of product in the past, or expressed an interest in a certain category of goods.[50] Or a political candidate might purchase a mailing list of voters who are registered to vote in that candidate's primary, or who have contributed to similar campaigns; those voters are good targets because they are likely to share the candidate's positions and have demonstrated a willingness to fund similar campaigns. Even people who have fallen for a scam once can be a promising target for further scams of the same kind.[51] Other targeting methods are subtler, as when a marketer targets people whose psychological profiles might make them susceptible to a pitch. For decades, magazines contained ads for nose-hair trimmers and other embarrassing products not because the sellers made money selling them but because someone with enough self-regard to want a nose-hair trimmer, but embarrassed enough not to buy it in a store, turns out to be a great target for other products.[52] Modern direct-mail targeting can be incredibly sophisticated (and correspondingly expensive). Target, for instance, got a lot of attention when it used its extensive information on individual shoppers' purchases to infer which customers had recently become pregnant, so it could mail them coupons for baby stuff.[53]

Three pieces of modern technology have transformed targeted advertising, making it easier and cheaper to target individual consumers without going to the trouble of building a list or using the mail.[54] First, much more information is available about

50. *See, e.g.*, *Miller Asks Court to Order List Broker to Respond to Telemarketing Fraud Probe*, IOWA DEP'T JUST. (Mar. 3, 2005), https://www.iowaattorneygeneral.gov/newsroom/miller-asks-court-to-order-list-broker-to-respond-to-telemarketing-fraud-probe [https://perma.cc/9C6L-6YT6] (claiming that list broker Walter Karl, Inc. sold lists described as containing "avid sweepstakes players, . . . sweepstakes enthusiasts[,] . . . cash-hungry individuals, impulsive buyers . . . primarily mature, hard core sweeps fanatics, credit-seeking individuals . . . looking . . . for ways to regain a good credit standing, and sweepstakes contestants over the age of 40, with household income of approximately $25,000," which were allegedly used for illegal telemarketing scams).

51. *E.g.*, Jason Cossman, *The Stoned Leading the Blind*, HARPER'S MAG., June 2008, at 1, 20 (describing a scam by which essentially identical products are sold under two different brand names, the first for an auto-renewing $84.50 a month, and the second to people who call to cancel the first).

52. *See, e.g.*, Frances Cole Jones, *A Perfect Business Model: Nose Hair Trimmers*, FORBES (Feb. 16, 2011, 2:17 PM), https://www.forbes.com/sites/work-in-progress/2011/02/16/a-perfect-business-model-nose-hair-trimmers/ [https://perma.cc/LPH5-GSQX].

53. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html [https://perma.cc/TL6A-NWFJ]; Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012, 11:02 AM), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/ [https://perma.cc/HKZ8-75DB].

54. For a useful overview of this transformation, see MIKE SMITH, TARGETED (2014).

individual consumers in the form of commercial datasets.[55] Most consumers are familiar with data collected for specific purposes like assessing creditworthiness, but the sheer number of companies goes far beyond the three major credit bureaus, with thousands of largely unregulated data brokers maintaining—and selling access to—files on individual consumers.[56] Second, increases in computer processing and storage capabilities have made it easier and cheaper to process this information to draw inferences. With a sufficiently comprehensive dataset, then, a company can determine which consumers are most likely to be receptive to a specific piece of advertising.[57] Third, online targeting platforms have productized and commoditized targeting—turned what was an expensive service or task requiring custom internal work into one sold as a standard product[58]—so that advertisers can use individualized targeting without substantial investments of time, money, or expertise.[59] Some of these platforms, like Google

---

For a representative how-to guide on ways to take advantage of the transformation, see, for example, IAN DODSON, THE ART OF DIGITAL MARKETING (2016). For discussions of how these targeting techniques have been used in election campaigning—including before the Russian government used Twitter and Facebook targeting to troll the 2016 presidential election—see EITAN D. HERSH, HACKING THE ELECTORATE 66–87 (2015); SASHA ISSENBERG, THE VICTORY LAB 272–75 (2012); DANIEL KREISS, PROTOTYPE POLITICS 204–20 (2016), and also Sheera Frenkel & Katie Benner, *To Stir Discord in 2016, Russians Turned Most Often to Facebook*, N.Y. TIMES (Feb. 17, 2018), https://www.nytimes.com/2018/02/17/technology/indictment-russian-tech-facebook.html [https://perma.cc/XKZ4-J9RW] ("Facebook built incredibly effective tools which let Russia profile citizens here in the U.S. and figure out how to manipulate us.").

55. *See, e.g.*, STAFF OF S. COMM. ON COMMERCE, SCI., & TRANSP., 113TH CONG., A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES 13–21 (2013); FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 13–15 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/J9D4-PZWH].

56. On the estimate that there are thousands of data brokers, see Susan Moore, *How to Choose a Data Broker*, GARTNER (June 8, 2016), https://www.gartner.com/smarterwithgartner/how-to-choose-a-data-broker/ [https://perma.cc/8UYC-C3Q5] ("Gartner estimates there may be up to 5,000 data brokers . . . worldwide, plus nearly 10 million open datasets published by government agencies and non-governmental organizations (NGOs).").

57. Cambridge Analytica, the analytics firm that worked with the Trump campaign in 2016, for instance, claimed that it developed psychological profiles of 230 million Americans from data taken from Facebook profiles. Carole Cadwalladr, *'I Made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower*, GUARDIAN (Mar. 18, 2018, 9:44 AM), https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump [https://perma.cc/CA5Z-SN8U].

58. *See* Dennis Kennedy, *Subscription Offer*, A.B.A. J., Apr. 2015, at 1, 33; Mohanbir Sawhney, *Putting Products into Services*, HARV. BUS. REV. (Sept. 2016), https://hbr.org/2016/09/putting-products-into-services [https://perma.cc/28P5-MG7N].

59. Facebook advertising, for instance, requires a minimum budget of just 50¢ or $1 a day, depending on the currency used. *See Ads Help Center: About Minimum Budgets*, FACEBOOK BUS., https://www.facebook.com/business/help/203183363050448 [https://perm

and Facebook, are familiar to users, while others, like the ad networks deploying the thousands of tracking tools blocked by various browser extensions, are less well known.[60] All of them have helped transform targeted advertising from a sophisticated and expensive endeavor requiring substantial effort to one that is available to advertisers of all sizes and levels of sophistication.

Modern individualized targeting may or may not require connecting a profile to a real-world identity, which means the implications for consumers are not uniform. Some forms of targeting use profiles of individual, identifiable users and cannot work without those profiles. Most targeted direct mail works this way; credit-card companies, for instance, solicit individuals with specific credit profiles, which requires linking information about creditworthiness to names and addresses.[61] Likewise, political campaigns build detailed profiles of individual voters, which they

---

a.cc/NK6W-W7MF] (last visited Sept. 12, 2019).

60. These trackers work by referencing third-party resources in a webpage's code; the New York Times website, for instance, might load an ad from servers run by DoubleClick, a Google subsidiary that places online ads. The user's browser, when it reads and executes that code, will reach out to the DoubleClick server asking for an ad. If DoubleClick has previously placed a cookie on the computer with a unique ID number, the browser will also generally provide that ID number. Because more than one website uses DoubleClick to serve ads, DoubleClick can develop a profile of that user across multiple websites. These third-party resources can have many different uses; some, like font or commenting services, provide important functionality for users, while others, like trackers and ad servers, are things a user might want to block. Dozens of such plugins have popped up, typically using databases of known trackers to decide which third-party resources should be blocked. For instance, as of August 30, 2019, the database used by the Ghostery plugin contains over 4,500 trackers, broken up into categories like "advertising," "site analytics," "audio/video player," and "adult content and comments." *See* Brian Barrett, *Ghostery Deploys AI in the Fight Against Ad Trackers*, WIRED (Dec. 5, 2017, 9:55 AM), https://www.wired.com/story/ghostery-deploys-ai-in-fight-against-ad-trackers/ [https://perma.cc/9TE6-868T]; *How Are Ghostery Lite Tracker Categories Defined and Maintained?*, GHOSTERY, https://www.ghostery.com/faqs/how-are-ghostery-lite-tracker-categories-defined-and-maintained/ [https://perma.cc/BB9V-NQCU] (last visited Sept. 12, 2019); *How Many Trackers Does Ghostery Have in Our Library?*, GHOSTERY, https://www.ghostery.com/faqs/many-trackers-ghostery/ [https://perma.cc/94DU-U5NW] (last visited Sept. 12, 2019). A competitive market for blocking plugins has emerged on several platforms; for others, see, for example, ADBLOCK PLUS, https://adblockplus.org/ [https://perma.cc/FD9F-FBU5] (last visited Sept. 12, 2019); John Corpuz, *Best Ad Blockers and Privacy Extensions*, TOM'S GUIDE, https://www.tomsguide.com/us/pictures-story/565-best-adblockers-privacy-extensions.html [https://perma.cc/YAR6-PA8Y] (last visited Sept. 12, 2019); *Privacy Badger*, EFF, https://www.eff.org/privacybadger/ [https://perma.cc/V56T-PKUK] (last visited Sept. 12, 2019). Tracker-blocking plugins have also made the leap from desktop web browsers to phones and tablets. *See, e.g.*, Mike Shields, *Apple Software Update Brings Ad Blockers Along with Apple News Sponsors*, WALL ST. J.: CMO TODAY (Sept. 16, 2015, 3:50 PM), https://blogs.wsj.com/cmo/2015/09/16/apple-software-update-brings-ad-blockers-along-with-apple-news-sponsors/ [https://perma.cc/L6E6-VFD5].

61. *See Prescreened Credit and Insurance Offers*, FED. TRADE COMM'N (Mar. 2011), https://www.consumer.ftc.gov/articles/pdf-0035-prescreened-credit-and-insurance-offers.pdf [https://perma.cc/583F-QJGX].

can use to ask those voters for donations, choose the campaign literature most likely to persuade them, and help know who to focus on getting out to the polls.[62] Other forms of targeting, though, work even if no individual identity is ever tied to the profile. This is behavioral advertising, and most online targeting works this way, with ad networks using random ID numbers to build demographic profiles that need not be connected to any real-world identity. An ad network might infer, for instance, based on browsing history that user number 82332943 spends time on sites about video games, action movies, and car racing, while user 82332944 is more interested in luxury travel, fashion, and financial services. The ad network can use that info to show relevant ads without ever linking those profiles to specific people.

The shift from indirectly to directly targeted advertising has two major effects. The first is the efficiency gain discussed above; to the extent targeting lets advertisers avoid showing their ads to people not in the right groups, it can save money. The second effect is that direct targeting requires collecting and using a lot of information about individual users, which necessarily leads to privacy losses. This is a substantial effect, but one I will largely set to the side in this Article.[63]

Notably, though, the efficiency gains from targeted advertising can be more complicated than the simple story would indicate, for several reasons. For one, only some kinds of

---

62. *See* ISSENBERG, *supra* note 54, at 56–63; Bill Lambrecht, *Trump's Digital Ad Exec Based in San Antonio*, SAN ANTONIO EXPRESS-NEWS (Nov. 15, 2016), https://www.expressnews.com/news/local/article/Trump-s-digital-ad-exec-based-in-San-Antonio-10616777.php [https://perma.cc/2YAJ-UX8M] (quoting Brad Parscale, who ran digital operations for the 2016 Trump campaign and has been named as campaign manager for the 2020 reelection bid: "Maybe you see an ad on Facebook and donate $5. Now you're in my system. So now it doesn't become efficient for me to get money from you on Facebook because they charge me. So I start using other means; cellphone, email and other operations to get to you to make further donations."); Issie Lapowsky, *Here's How Facebook Actually Won Trump the Presidency*, WIRED (Nov. 15, 2016, 1:12 PM), https://www.wired.com/2016/11/facebook-won-trump-election-not-just-fake-news/ [https://perma.cc/72YE-4FX5]; Tim Mak, *Trump Names 2020 Campaign Manager*, NPR (Feb. 27, 2018, 2:08 PM), https://www.npr.org/2018/02/27/589210484/trump-names-2020-campaign-manager [https://perma.cc/Q5N7-XLNB].

63. For just a bit of the voluminous work on the privacy issues presented by targeted advertising and individualized targeting, see, for example, DANIEL J. SOLOVE, THE DIGITAL PERSON (Jack M. Balkin & Beth Simone Noveck eds., 2004); Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241 (2007); David S. Evans, *The Online Advertising Industry: Economics, Evolution, and Privacy*, J. ECON. PERSP., Summer 2009, at 37; Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606 (2014); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998); Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907 (2013); Katherine J. Strandburg, *Free Fall: The Online Market's Consumer Preference Disconnect*, 2013 U. CHI. LEGAL F. 95.

advertising benefit from targeting. Advertising to niche communities, for instance, may be impossible without targeting. But in other cases, advertising requires wide distribution to work in the first place. Ads for major consumer brands like Coca-Cola and Apple aim for scale and widespread distribution since those firms try to sell their products to as many people as possible, so there's little benefit to targeting. Likewise, even companies trying to sell their products to limited audiences, like makers of luxury goods, may depend on brand cachet and awareness to generate a sense of exclusivity.[64]

When a narrow audience is desired, the gains from targeting can be muted for other reasons. For one, the fact that targeting can make advertising more efficient doesn't tell us *how much* more efficient that is; if targeting produces a 20% gain in advertising efficiency, that's a different story than if it produces a 2% gain or a 0.2% gain. There's surprisingly little research on the question, likely because the parties in the best position to know—the targeting platforms themselves—have good reason to protect those numbers as trade secrets.[65]

Targeting can also be counterproductive for advertisers, offsetting the efficiency gains. This is so because some consumers don't like it when advertising appears to be targeted, which can appear creepy and highlight the amount of information

64. *See, e.g.*, JEAN-NOËL KAPFERER & VINCENT BASTIEN, THE LUXURY STRATEGY 69–70 (2009). Indeed, one of Kapferer and Bastien's "anti-laws" of luxury marketing is "[c]ommunicate to those whom you are not targeting," because "[i]n luxury, if somebody is looking at somebody else and fails to recognize the brand, part of its value is lost." *Id.*

65. Part of the trouble is that the right metric would compare targeted advertising not to purely untargeted advertising, but to indirect forms of targeting like contextual advertising. When an ad matches the context in which it appears—when car ads appear on car websites or search-engine ads are based on the keywords searched, for instance—it should provide many of the benefits of targeting without the need to build user profiles or the attendant privacy risks. Many of the studies evaluating targeted advertising compare it instead to untargeted advertising like run-of-network advertising, in which an ad appears randomly across an ad network's inventory. *E.g.*, J. HOWARD BEALES & JEFFREY A. EISENACH, AN EMPIRICAL ANALYSIS OF THE VALUE OF INFORMATION SHARING IN THE MARKET FOR ONLINE CONTENT 8–15 (2014), https://ssrn.com/abstract=2421405 [https://perma.cc/WE27-GFPP]; HOWARD BEALES, THE VALUE OF BEHAVIORAL TARGETING 6–17 (2010), https://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf. [https://perma.cc/54M4-3KLR] The most prominent study found that advertising effectiveness fell sharply in Europe after the E.U. Privacy Directive limited the ability of companies to build user profiles, suggesting that targeting was responsible for much of the value of web ads. Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, 57 MGMT. SCI. 57, 58, 69–70 (2011). That result, though, is hard to evaluate given the small effect size of ads both before and after the Privacy Directive; the authors also found that the effect is mitigated by using contextual advertising instead of run-of-network advertising. *See* Strandburg, *supra* note 63, at 102–05.

advertisers have about people.[66] So when companies use targeting in ways that consumers can perceive, the privacy losses can undo the efficiency gains from targeting. Target, for instance, saw this when it figured out how to tell if a customer was pregnant. The company used that information to send coupons for baby stuff, backfiring spectacularly when customers found it incredibly creepy to get a "congratulations on your upcoming baby!" mailing from a giant faceless corporation. Sometimes a customer had lost the pregnancy; sometimes a customer was a teenager whose parents found out about the pregnancy from Target; sometimes they just found it creepy. Whatever the reason, customers didn't respond by buying baby stuff from Target—until the company found an ingenious loophole. Instead of sending pregnant customers baby-themed mailings, they would just send a packet of seemingly unrelated coupons, with some baby-themed ones sprinkled in among decoy coupons. That worked.[67] The effect is not unique to Target and mail-order coupons; the same can be true online, as when a user shops for a specific product and then sees ads for that product on other websites.[68] Marketers must be careful, then, not to go too far in using consumer data to target their ads.

Even when targeting works for an advertiser, the same interdependence between privacy and efficiency holds for society as a whole. Targeting might make advertising work better, allowing platforms and advertisers to make more money. It might also provide benefits for consumers, who get free content and learn about goods and services that are relevant to their interests. But

66. *See* Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 66–69 (2013).

67. *See* Duhigg, *supra* note 53; Hill, *supra* note 53.

68. For instance, Avi Goldfarb and Catherine Tucker found that two distinct interventions—making the ad more targeted and more obtrusive—each individually increased the effectiveness of online advertising, but when combined, they decreased the ads' effectiveness. They attributed this difference to privacy concerns: obtrusive ads that appeared targeted were counterproductive, with the biggest drops in effectiveness coming from users who refused to give their income and for categories where privacy concerns were especially salient. They concluded that their results could explain why the market for online advertising is increasingly bifurcated into highly targeted text ads and "more visually striking but less targeted ads." Avi Goldfarb & Catherine Tucker, *Online Display Advertising: Targeting and Obtrusiveness*, 30 MARKETING SCI. 389, 400 (2011). In another experiment, Anja Lambrecht and Catherine Tucker found that targeted travel ads—ads showing specific hotels that the targeted users had previously looked at—were less effective than generic hotel ads. This effect, though, didn't seem to be driven by privacy, but instead by consumers going through multiple stages of shopping, since targeted ads became more effective after users had visited a review site, indicating that they were specifically interested in those hotels. Anja Lambrecht & Catherine Tucker, *When Does Retargeting Work? Information Specificity in Online Advertising*, 50 J. MARKETING RES. 561, 573–575 (2013).

it also creates privacy costs—costs that are largely borne by consumers and the rest of society, not by platforms and advertisers. Just as privacy concerns might blunt the effectiveness of targeting in the individual case, privacy harms might offset the social benefits of targeting.

A realistic account of online targeting and online advertising, then, is more nuanced than the simple efficiency-versus-privacy story might indicate. Targeting can make advertising more efficient, which can be a good thing when advertising is a good thing. These gains are offset, however, both by the costs of privacy losses for consumers and for society and by the ways that targeting can reduce the effectiveness of advertising in the first place. Moreover, this conventional view doesn't account for other effects of online targeting, like making it easier to perpetuate scams, as I discuss in the next Part.

III. DATA SCAMS

For as long as there has been human civilization, there have been people who try to take unfair advantage of others. These scams take countless forms, from outright frauds to subtler schemes that may or may not violate the law. Though they are nothing new, many of these scams become easier to perpetuate, and harder to detect and prevent, due to the targeting tools discussed above. This Part discusses how data affects scams, first reviewing different kinds of scams and then discussing how modern targeting changes things for scammers and those trying to detect and prevent scams.

A. Scams

"Scam"—like "privacy," "design," and a lot of other terms that play important roles in modern technology law—is a broad and imprecise word that can encompass many kinds of behavior. I use the word instead of one with a more-specific meaning, like fraud, because there are many kinds of scams, with many different elements, that can be perpetuated online. Some involve lying to their victims, for instance, but others might tell the truth but prey on other vulnerabilities to take advantage.

In this Article, I use the term to describe a wide variety of frauds, schemes, rip-offs, flimflams, tricks, and other dirty businesses or transactions. There are two critical elements and one nonelement, each discussed below. First, a scam is an effort to *take advantage* of a victim. This can be characterized in several ways: maybe a scammer manipulates or deceives a victim or presents her with unfair choices. In general, though, a victim of a

scam makes a seemingly voluntary choice to act in a way that benefits the scammer and harms her own interests.[69] Second, this means that a scam involves two participants: a scammer who perpetuates the scam and benefits from it, and a victim who is harmed (or intended to be harmed) by it. This separates scams from ordinary market transactions in which both participants benefit, even though some such transactions will involve deception or some other scam-like behavior along the way.[70] Third, neither of these elements requires the scam to be illegal. While some scams clearly violate criminal law or constitute civil wrongs, others might be legal or might not have been addressed definitively by courts and policy makers.

1. Taking Advantage. The fundamental nature of a scam is that it takes advantage of someone. Scammers seek to do this by causing the victim to act contrary to her own interests.[71] There are lots of ways to do this—lying to, or deceiving, a victim; appealing to her emotions; exploiting various cognitive biases; maybe making it easier to make a dumb choice than a smart one—but for all of them, the goal is to get the victim to do something or give up something that benefits the scammer. A scam, then, would not work if the victim had full information and acted rationally.

There are different ways to characterize a scammer's actions, and no single vocabulary has yet developed to describe a phenomenon that turns out to be fairly widespread. The law has its own language: criminal law bans *frauds* and *schemes* or *artifices to defraud* in a variety of contexts,[72] while the Federal Trade Commission is charged with going after *deceptive* and *unfair*

69. Scams, then, are a subset of what economists call "demerit goods," like cigarettes or liquor, which are overconsumed due to imperfect knowledge or other market failures. *See, e.g.*, RICHARD A. MUSGRAVE & PEGGY B. MUSGRAVE, PUBLIC FINANCE IN THEORY AND PRACTICE 328–29 (2d ed. 1976); John G. Head, *On Merit Goods*, 25 FINANZARCHIV 1, 3 (1966) (Ger.).

70. Consider a buyer negotiating a purchase who says that an offer is as low as they can go, or a seller who says another buyer is interested in the item, when those things are not in fact true.

71. In one sense, a victim of a scam acts voluntarily; this separates scams from simple crimes or torts like theft or assault. Though this view raises critical questions about what it means to act voluntarily when cognitive biases and failures cause people to act in predictably irrational ways.

72. In the federal system, see, for example, 18 U.S.C. § 1341 (2012) (mail fraud); *id.* § 1343 (wire fraud); *id.* § 1344 (bank fraud); *id.* § 1347 (health-care fraud); *id.* § 1348 (securities and commodities fraud). In the states, see, for example, N.Y. PENAL LAW §§ 170.00–190.89 (McKinney 2019) (Title K, "offenses involving fraud"). Fraud is itself a term with a lot of meanings, but the essence focuses on dishonesty, requiring an intentional or reckless misrepresentation or concealment of a material fact to induce another to act to her detriment. *See Fraud*, BLACK'S LAW DICTIONARY (10th ed. 2014).

trade practices.[73] Other fields have weighed in too. The philosophers Daniel Susser, Beate Roessler, and Helen Nissenbaum identify and describe *manipulation* as "imposing a hidden or covert influence on another person's decision-making," which they contrast with other forms of influence like persuasion and coercion.[74] The economists George Akerlof and Robert Shiller use *phishing* as a term for ways of "getting people to do things that are in the interest of the phisherman, but not in the interest of the target."[75] They borrow the term from internet scams designed to obtain personal information but argue by analogy that it can apply to a broad array of scams in a variety of contexts. And the legal scholar Brett Frischmann and philosopher Evan Selinger talk about tools and technology being used to "re-engineer" humans, like when companies manipulate their workplaces to encourage productivity or schools distribute fitness trackers to encourage exercise (normalizing surveillance in the process).[76]

These are all variations on a theme. In each of these conceptions, a scammer uses any of a variety of tools to take advantage of a victim to act in a way that benefits the scammer. And in all of them, courts and scholars have cautioned against narrowly drawn definitions, instead interpreting terms flexibly to cover a variety of scams.

The federal mail- and wire-fraud statutes, for instance, leave "scheme or artifice to defraud" undefined, and courts have consistently declined to provide a more-precise definition.[77] Courts

73. *See* 15 U.S.C. § 45(a)(2).

74. Susser et al., *supra* note 6, at 22; *see also* Daniel Susser et al., *Technology, Autonomy, and Manipulation*, INTERNET POL'Y REV., June 30, 2019, at 1, 3–4. For related discussions of manipulation, see, for example, Cass R. Sunstein, *Fifty Shades of Manipulation*, 1 J. MARKETING BEHAV. 213, 218 (2015); Tal Z. Zarsky, *The Problem of Theorizing Privacy: Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRIES L. 157, 169–74 (2019).

75. GEORGE A. AKERLOF & ROBERT J. SHILLER, PHISHING FOR PHOOLS xi (2015) (describing the origins of, and drawing an analogy to, the term phishing in the Internet context).

76. BRETT FRISCHMANN & EVAN SELINGER, RE-ENGINEERING HUMANITY 17–28, 53–59 (2018).

77. Courts have been far more willing to define and limit the kinds of benefits that can give rise to fraud liability. In *McNally v. United States*, for instance, the Supreme Court limited the mail- and wire-fraud statutes to efforts to obtain money or other forms of property. McNally v. United States, 483 U.S. 350, 358–60 (1987). Congress responded by expanding those crimes to cover a "scheme or artifice to deprive another of the intangible right of honest services." 18 U.S.C. § 1346. The Supreme Court has interpreted that provision narrowly, though, holding that it applies only when a defendant receives bribes or kickbacks, thereby defrauding the defendant's employer or (in the case of an elected official) voters. Skilling v. United States, 561 U.S. 358, 404–13 (2010). The fact that the money or property in such a scheme came from a third party rather than from the defrauded

generally expect some element of deception or dishonesty, but that is not especially limiting, as the Fifth Circuit explained in *Gregory v. United States*: "The aspect of the scheme to 'defraud' is measured by nontechnical standard. It is a reflection of moral uprightness, of fundamental honesty, fair play and right dealing in the general and business life of members of society."[78] A wide variety of scams, then, have been found to fall within the statutes. In *Gregory*, for instance, the defendant used backdated postmarks to mail entries in a contest to predict college-football scores and win a Cadillac.[79] The postmarks suggested that the picks had been mailed by the midweek deadline before the weekend's games, when instead they had been filled out after the games had been played.[80] The Court had no trouble finding mail fraud because the defendant "found a way to gain an advantage" by "pretend[ing] that his prediction was . . . made and mailed by" the deadline.[81] The lack of a single affirmative false statement did not matter.[82] At the same time, other cases find that even concededly false statements or concededly material omissions do not amount to fraud when a reasonable counterparty would not rely on the statement or omission.[83]

The Federal Trade Commission Act's prohibition on deceptive and unfair trade practices is even more expansive in the sheer scope of prohibited activities, though it's limited to commercial practices. Under section 5 of the Act, "unfair or deceptive acts or practices in or affecting commerce" are unlawful and subject to the FTC's enforcement authority.[84] The terms are intentionally broad and vague, giving the FTC substantial enforcement discretion.[85]

---

party—that the transaction had three parties instead of two—didn't matter, the Court explained. *Id.* at 410. It was still a scheme to obtain money or property and so covered by the statutes. *Id.*

78. Gregory v. United States, 253 F.2d 104, 109 (5th Cir. 1958). *But see In re* EDC, Inc., 930 F.2d 1275, 1281 (7th Cir. 1991) (rejecting the "hyperbole" of *Gregory* and asserting that "[r]ead literally it would put federal judges in the business of creating new crimes; federal criminal law would be the nation's moral vanguard").

79. *Gregory*, 253 F.2d at 106–07.

80. *Id.* at 106.

81. *Id.* at 109.

82. *Id.*

83. *E.g.*, United States v. Weimert, 819 F.3d 351, 357–58 (7th Cir. 2016); Reynolds v. E. Dyer Dev. Co., 882 F.2d 1249, 1252–53 (7th Cir. 1989); United States v. Kwiat, 817 F.2d 440, 445–46 (7th Cir. 1987).

84. Federal Trade Commission Act, Pub. L. No. 63-203, ch. 311, § 5, 38 Stat. 717, 719 (1914) (codified as amended at 15 U.S.C. § 45(a)(1)–(2) (2012)).

85. FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 239–40 (1972); Atl. Ref. Co. v. FTC, 381 U.S. 357, 367 (1965); FTC v. Bunte Bros., 312 U.S. 349, 353 (1941); FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 243 (3d Cir. 2015); *see also* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION: PRIVACY LAW AND POLICY 119–20 (2016)

Though the Act does not define "deceptive," the FTC explained in a policy statement that it requires a "representation, omission or practice that is likely to mislead the consumer."[86] The Act also specifies that a practice can only be unlawful as "unfair" if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[87] Beyond those constraints, Congress has allowed the FTC to develop a body of law interpreting "unfair or deceptive acts or practices" through enforcement actions, including settlements.[88]

Through this history of enforcement, the FTC has found many kinds of actions to be deceptive or unfair. Classic deceptions include false or misleading statements or implications, for instance about a product's price, quality, or features.[89] In the contexts of privacy and data security, the FTC extended these cases to cover false promises to protect users' private information, or false implications that the company will do so;[90] trickery like telling people they need to download a piece of malicious "security" software or disclose confidential information when they don't really need to do so;[91] disclosures of privacy practices that are

(noting that Congress intentionally chose vague language in 1914 and 1938 "because business practices and technology were constantly evolving, causing new problems that Congress could not quickly act to remedy").

86. Letter from James C. Miller III, Chairman, FTC, to John D. Dingell, Chairman, House Comm. on Energy & Commerce (Oct. 14, 1983), *reprinted in* Cliffdale Assocs., Inc., 103 F.T.C. 110 app. at 174–75 (1984) (decision & order).

87. 15 U.S.C. § 45(n); *see also Sperry & Hutchinson Co.*, 405 U.S. at 244 n.5; LabMD, Inc. v. FTC, 894 F.3d 1221, 1227–29 (11th Cir. 2018) (suggesting, in dictum, that this statutory definition might add to, rather than supplant, previous FTC interpretations requiring that an allegedly unfair trade practice "offend[ ] public policy as established by statute, the common law, or [the Constitution]") (citing Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8355 (July 2, 1964) (codified at 16 C.F.R. § 408)).

88. *See, e.g.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 606–08 (2014) (arguing that the FTC's privacy enforcement actions, and especially its settlements, have developed a body of law akin to a common law of privacy).

89. Letter from James C. Miller III, *supra* note 86, app. at 182–83; *see also* 1 STEPHANIE W. KANWIT, FEDERAL TRADE COMMISSION § 4.04 (2018).

90. *See* Solove & Hartzog, *supra* note 88, at 628–30; *see also, e.g.*, *Wyndham Worldwide Corp.*, 799 F.3d at 240–42 (lawsuit alleging that Wyndham used inadequate data-security practices, in violation of promises to protect customers' information, leading to a data breach); *LabMD, Inc.*, 894 F.3d at 1224–29 (similar); Eli Lilly & Co., 133 F.T.C. 763, 766–68 (2002) (complaint alleging that Eli Lilly disclosed customers' personal information in violation of privacy policy).

91. *E.g.*, FTC v. Ross, 743 F.3d 886, 889–90 (4th Cir. 2014) (affirming judgment in favor of the FTC when defendants ran ads claiming that victims' computers had been scanned and were infected with malware when in fact no scans had been run); Default

inadequate or too vague to meaningfully inform consumers about how their data is used;[92] and even failure to follow industry standards when a company's statements and behavior otherwise implied that they will do so.[93] Actions the FTC has found to be unfair include hiding price information to make it hard to compare prices across vendors;[94] bringing creditor lawsuits in distant and inconvenient forums;[95] refusing to refund the value of repossessed cars beyond the amount owed on a bad car loan;[96] designing

---

Judgment and Order for Permanent Injunction and Monetary Judgment as to Defendant Innovative Marketing, Inc. at 2–5, FTC v. Innovative Mktg., Inc., No. 08-CV-3233-RDB (D. Md. Feb. 24, 2010) (order granting default judgment on similar facts); First Amended Complaint for Injunctive and Other Equitable Relief at 2, 6–8, FTC v. Enternet Media, Inc., No. CV05-7777 CAS (C.D. Cal. Nov. 4, 2005) (seeking a temporary restraining order when defendants distributed code to embed free-music widgets in webpages, when the widgets also offered to "upgrade" users' browsers and actually installed spyware).

92. *E.g.*, Complaint at *7–9, Facebook, Inc., No. C-4365, 2011 WL 7096348 (F.T.C. Nov. 29, 2011) (complaint alleging that Facebook's Privacy Wizard did not adequately disclose that users could no longer restrict access to certain information and that previous decisions to do so would no longer be honored); Complaint at *2–7, Google Inc., No. C-4336, 2011 WL 5089551 (F.T.C. Oct. 13, 2011) (complaint alleging that Google's privacy policies and the setup process for a Google Buzz account were too vague to place users on notice that certain information would be publicly shared by default); *see also* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 27 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/92HE-7NRK] ("The Commission recognizes the need for flexibility to permit innovative new uses of data that benefit consumers. At the same time, in order to protect consumer privacy, there must be some reasonable limit on the collection of consumer data. General statements in privacy policies, however, are not an appropriate tool to ensure such a limit because companies have an incentive to make vague promises that would permit them to do virtually anything with consumer data.").

93. *E.g.*, *Wyndham Worldwide Corp.*, 799 F.3d at 241 (lawsuit alleging that Wyndham falsely claimed that "[w]e safeguard our Customers' personally identifiable information by using industry standard practices"); Complaint at *3–5, Uber Techs., Inc., File No. 152-3054, 2017 WL 3621176 (F.T.C. Aug. 15, 2017) (complaint alleging that Uber repeatedly falsely stated and implied that it used state-of-the-art industry-standard security practices, allowing an intruder to gain access to user data hosted on Amazon cloud servers).

94. *E.g.*, Funeral Industry Practices, 16 C.F.R. §§ 453.1–453.2 ("In selling or offering to sell funeral goods or funeral services to the public, it is an unfair or deceptive act or practice for a funeral provider to fail to furnish accurate price information disclosing the cost to the purchaser for each of the specific funeral goods and funeral services used in connection with the disposition of deceased human bodies . . . to persons inquiring about the purchase of funerals.").

95. Spiegel, Inc. v. FTC, 540 F.2d 287, 291, 293–94 (7th Cir. 1976) (holding that the FTC could find it unfair to sue consumers in distant and inconvenient forums even when the forums had jurisdiction over the cases).

96. *E.g.*, *In re* Gen. Motors Corp., [1979–1983 Transfer Binder] 12 Trade Reg. Rep. (CCH) ¶ 21,665 (F.T.C. June 11, 1980) (proposing to create a $2 million fund for consumers whose cars were repossessed and did not receive any surplus owed); *In re* Ford Motor Co., [1976–1979 Transfer Binder] 12 Trade Reg. Rep. (CCH) ¶ 21,477 (F.T.C. Oct. 15, 1978) (requiring this surplus to be paid within forty-five days).

software that made it unduly difficult for users to protect their privacy;[97] and, again, failure to follow industry data-security standards.[98]

Though they use a variety of linguistic formulations, academics in several fields have likewise focused on actions that take advantage of victims in these ways. Susser, Roessler, and Nissenbaum, for instance, start with three disparate problems—targeted advertising aimed at teenagers, gig-economy platforms like Uber that nudge their workers to do things that benefit the platform, and the use of detailed personality profiles in election targeting—and argue that they are examples of the same phenomenon, manipulation.[99] They define manipulation as "imposing a hidden or covert influence on another person's decision-making . . . . by targeting and exploiting their cognitive, emotional, or other decision-making vulnerabilities" and conclude that it differs from other ways of affecting someone's decision, like persuasion and coercion.[100] In persuasion, one offers arguments or incentives to try to get a decision maker to make a preferred choice; in coercion one eliminates all but the desired option. Both of these tools, then, are in some sense *honest* means of getting someone to act: the decision maker understands what options are available and can make a choice or not, with full knowledge of the choices. With manipulation, though, the manipulator subverts this capacity for self-government through some sort of hidden influence, unknown to the decision maker. This can be as simple as lying or deceiving the decision maker, so that she acts on the basis of information that is incomplete or wrong. But there are other ways to manipulate someone. Susser, Roessler, and Nissenbaum highlight manipulations that take advantage of cognitive biases or forms of bounded rationality, or that capitalize on other "psychological levers," like people's individual emotions or desires.[101]

Akerlof and Shiller's description of "phishing,"[102] likewise, shares much with the Susser, Roessler, and Nissenbaum

97. *E.g.*, Complaint ¶¶ 25–32, FTC v. FrostWire LLC, No. 1:11-cv-23643 (S.D. Fla. Oct. 7, 2011) (alleging that FrostWire designed its file-sharing software to make it unfairly difficult for consumers to avoid sharing certain categories of personal files by requiring them to opt out on a file-by-file basis); Stipulated Final Order for Permanent Injunction, FTC v. FrostWire LLC, No. 11-23643-CV-GRAHAM (S.D. Fla. Oct. 12, 2011) (stipulated permanent injunction).

98. *E.g.*, *Wyndham Worldwide Corp.*, 799 F.3d at 246–49.

99. Susser et al., *supra* note 6, at 3–9.

100. *Id.* at 22.

101. *Id.* at 15, 18.

102. AKERLOF & SHILLER, *supra* note 75, at xi.

description of manipulation and the account of scams I develop here. The classic form of phishing on the internet is a scam where someone sends an e-mail pretending to be from a major company or bank, hoping the recipient will provide real login information on a fake login page. Akerlof and Shiller generalize the term:

> It is about getting people to do things that are in the interest of the phisherman, but not in the interest of the target. It is about angling, about dropping an artificial lure into the water and sitting and waiting as wary fish swim by, make an error, and get caught.[103]

Like manipulation, phishing takes advantage of a victim's error and induces that error through lying or deception or just taking advantage of cognitive biases or emotions. Akerlof and Shiller do go farther, arguing that someone can phish even when nothing is hidden from the victim, though the difference is largely one of degree rather than kind.[104] Gambling addiction is a key example: An addict might know intellectually exactly what was going on but be emotionally incapable of stopping. Because casinos can design and select slot machines and games that capitalize on, and reinforce, whatever levers lead one to become addicted, they represent a lure that seeks to take advantage of a vulnerable victim, even if the victim knows it.[105] The point applies more broadly, though, any time people's "real" tastes and their "monkey-on-the-shoulder" tastes diverge—which is pretty much always.[106]

The practices characteristic of scams can take many forms, but they all seek to take advantage of a victim by causing her to act contrary to her own interests. In the "Dinner with Trump" scam discussed in the introduction, for instance, the scam used two sources of deception to extract money from donors. The name of the website—dinnerwithtrump.org—suggested a prize that many people would assume could only be provided by the Trump campaign. The website's design also mimicked the campaign site's, suggesting an affiliation.[107] Even if a savvy consumer could have read the fine print and discovered that an unaffiliated PAC ran the site, the website was nevertheless apparently designed to solicit contributions from those who would voluntarily give to the Trump campaign. It took advantage of the natural and predictable

---

103. *Id.*

104. *Id.* at ix–xi.

105. *Id.*; *see also* NATASHA DOW SCHÜLL, ADDICTION BY DESIGN: MACHINE GAMBLING IN LAS VEGAS (2012).

106. *See* AKERLOF & SHILLER, *supra* note 75, at 20–22.

107. *Cf.* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 21–55 (2018) (explaining how visual design implicitly conveys messages to users).

assumptions made by those who saw the PAC's ads to cause people who would not want to donate money to the PAC to go ahead and do so. It caused donors to act, contrary to their natural preferences, by misleading them and capitalizing on limited attention and cognitive biases.

As the gambling example makes clear, the line between a scam and a normal transaction can be blurry. Just as regulators and academics haven't agreed on a single vocabulary for discussing scams, there is no universal agreement on when a transaction is scammy enough to cross that threshold. Is it a scam when a seller prices a good at $9.99 instead of $10? When the seller hires attractive salespeople? When the seller advertises a heavily discounted product but then steers interested consumers to more expensive options? When the seller claims the good is "top quality" when it's really average? When the seller targets inebriated buyers or provides free drinks? All of these practices have some of the hallmarks of scams, due to deception or some effort to capitalize on a cognitive bias or vulnerability. They're also all common, usually noncontroversial commercial practices. Yet it is not hard to imagine more problematic versions of each, and regardless, it matters less *which* specific practices amount to scams and more that *some* clearly do. When a company misleads consumers about a product's price, quality, or features, it can cause customers who would not otherwise have purchased the product to do so. When a hotel chain claims it keeps customers' information secure but really leaves it on an out-of-date computer that hasn't received security updates in three years, security-conscious customers who would otherwise seek to avoid the security risk might stay in the chain's hotels.[108] When the pharmaceutical industry seeks to keep prices opaque, customers can't easily find the cheapest pharmacy at which to fill a prescription, and so will pay more for their prescriptions.[109]

2. Scammers and Victims. A scam is a transaction (or an attempt to form a transaction) and so requires at least two parties, a scammer and a victim. Scammers come from all walks of life; their common feature is that they try to get something from others and choose scams as their mechanism to do so. If there is money to be made or advantage to be taken, simple economics suggest

108. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 241, 245–46 (3d Cir. 2015).

109. *See, e.g.*, Kaitlyn N. Dana et al., *Drug Pricing Transparency: The New Retail Revolution*, 52 HOSP. PHARMACY 155, 156, 158 (2017) (arguing that a payer's access to more transparent pricing information may improve autonomy and optimize pricing negotiations).

that someone will take it; scammers are just those who have chosen to do so.

Victims are more interesting because many scams rely on exploiting the vulnerabilities of their victims. Scams commonly target the elderly or poor, recent immigrants, international tourists, even children. There are two big reasons for this. Members of vulnerable populations are, in many cases, more likely than others to fall for a scam. At the same time, they can also be less likely to report the scam or otherwise respond after the scam, reducing the scammer's risk.

There are many reasons a victim might fall for a scam. The elderly, for instance, are disproportionately likely to suffer from declining mental capacity as conditions like Alzheimer's disease and dementia set in. They are also more likely to be widowed or have family that have moved away, which can make them vulnerable to emotional manipulation.[110] Immigrants and tourists, in contrast, can be vulnerable, not because they suffer from any conditions or impairments, but because they are less familiar with the language and culture of an area. When that's the case, a seemingly friendly hand can exploit their unfamiliarity with the culture. Victims may also be reluctant to report scams to authorities for fear of drawing attention to themselves.[111] Indeed, some victims may be vulnerable specifically because they have no redress. For instance, the customers of Ashley Madison, a dating site for married people looking to cheat, were targeted by scammers after the site's customer database was stolen and published.[112]

Tourists are a notable example of vulnerable victims, for two reasons. First, they demonstrate that the specific vulnerabilities used by scammers can be context-specific; everyone is vulnerable at one time or another. Second, they demonstrate the ways that

110. *See, e.g.*, Carolyn L. Dessin, *Financial Abuse of the Elderly*, 36 IDAHO L. REV. 203, 221 (2000); Shelby A.D. Moore & Jeanette Schaefer, *Remembering the Forgotten Ones: Protecting the Elderly from Financial Abuse*, 41 SAN DIEGO L. REV. 505, 517–19 (2004); Seymour Moskowitz, *Saving Granny from the Wolf: Elder Abuse and Neglect—The Legal Framework*, 31 CONN. L. REV. 77, 99–101 (1998).

111. *See, e.g.*, Mara H. Gottfried, *St. Paul Immigrants, Don't Be Afraid to Call Us, Police Say in 4 Languages*, TWIN CITIES PIONEER PRESS (Nov. 30, 2016, 5:11 PM), http://www.twincities.com/2016/11/30/st-paul-immigrants-dont-be-afraid-to-call-us-police-say-in-4-languages/ [https://perma.cc/B2TY-SQMR]. *But see* Mary Bowerman, *Woman Calls Police Over Drug Dealer's 'Outrageous' Price Hike*, USA TODAY (Jan. 31, 2017, 8:20 AM), http://www.usatoday.com/story/news/nation-now/2017/01/31/woman-calls-police-over-drug-dealers-outrageous-price-hike/97275774/ [https://perma.cc/6VTQ-3SF6].

112. *E.g.*, Aimee Picchi, *Ashley Madison Hack Leads to Scams, Extortion*, CBS MONEYWATCH (Aug. 24, 2015, 12:49 PM), https://www.cbsnews.com/news/scams-extortion-attempts-arising-from-ashley-madison-hack/ [https://perma.cc/NB7L-UFFM].

scams can rely on assumptions and context cues to trick their victims, rather than specific false claims. Because many people hesitate to ask too many questions or seem too skeptical, a scammer can take advantage of a victim's willingness to fill in the gaps and make assumptions about good faith.[113] A common travel scam, for instance, involves locals who offer to act as tour guides for foreign visitors. At the end of the day, they propose a tea ceremony or celebratory dinner or some other special meal at a local restaurant for which they can vouch. When the tourists get the bill at the end of the meal, it is much higher than it should be—often by multiple orders of magnitude.[114] The victim tourists are in an environment where they are out of their comfort zones, so the friendly face of a guide can make them feel at ease. Once they let down their guard, the tourist can make implicit assumptions based on prior experiences—that a restaurant charges reasonable prices or would go out of business; that a friendly guide wouldn't take them to an overpriced restaurant—only to get scammed. The tourist's vulnerabilities—not speaking the language, not knowing their way around, wanting to trust a friendly face—are used against them.

The need to target vulnerable victims can help explain some of the more inexplicable features of some scams. Nigerian e-mail scams, for instance, famously use broken English and stories of riches so implausible that it can be hard to imagine anyone falls for them. The math suggests, though, that this feature of the scam is key for it to work.[115] Sending spam e-mail is basically free, but interacting with a recipient who responds to the scam takes time. Consequently, scammers need to filter out as many false positives as they can.[116] By making their e-mails nakedly implausible, then, scammers deter all but the most truly gullible marks from responding—and those are precisely the recipients who are most likely to fall for the scam. Scammers can spend their time

113. *E.g.*, Kit Yarrow, *The Science of Why We Fall for Scams That Are So Obviously Scams*, MONEY (Nov. 11, 2016), http://money.com/money/4568127/scams-psychology-why-victims-fall-tech-support-irs-facebook/ [https://perma.cc/A8X7-A3S5] (quoting one victim who explained, "[i]n retrospect I can see that I just kept filling in blanks and making assumptions instead of challenging what I was hearing").

114. *E.g.*, Kelsey Blodget, *The 9 Surprising Travel Scams You Need to Know About*, OYSTER (Apr. 29, 2017), https://www.oyster.com/articles/45965-the-9-surprising-travel-scams-you-need-to-know-about/ [https://perma.cc/X84Y-PBF5].

115. CORMAC HERLEY, WHY DO NIGERIAN SCAMMERS SAY THEY ARE FROM NIGERIA? 11–12 (2012), https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/WhyFromNigeria.pdf [https://perma.cc/F6CQ-6LAA].

116. *Id.*

interacting with victims who might pay off instead of those who won't.

This reasoning is not limited to Nigerian e-mail scams or illegal scams in general; "legitimate" businesses use it as well. For instance, some car dealers use direct-mail flyers promoting contests with implausibly generous prizes that can only be won if a customer comes into a dealership.[117] Dealers use this form of ex post targeting or filtering to bring especially gullible customers into the business so they can sell them new cars. Savvy consumers, sensing an implausible offer, throw the flyers away; ones who are more likely to overpay for a car come in to see if they've won something.

There are many other vulnerabilities that scammers seek to exploit. Many victims are desperate, whether for financial reasons or health reasons or family reasons, looking for anything that might solve problems. Many victims let down their guard when dealing with authority figures, or expert figures like tech-support workers, or scammers pretending to be these things.[118] Many victims follow ordinary social cues, which scammers can exploit, like feeling obligated to repay previous favors or gifts or not to say no to polite requests. Many victims are bored or greedy or lonely. Some victims don't seem very vulnerable at all but fall victim to scams that exploit their exposure to risk. Many investment scams, for instance, target successful, middle-aged, financially literate professionals—people in the market for investment opportunities.[119] Indeed, some vulnerabilities don't even look like vulnerabilities; one study found that simply spending time in online chat rooms increased adolescents' vulnerability to

---

117. As one finance manager explained on a Reddit forum where salespeople answer car buyers' questions:

> [Dealers that send out these promotions are] probably looking to scrape the bottom of the market. These mailers aren't typically targeting the smartest buyers, they want the impulse shoppers and people who are easily swayed by shiny things. Most educated consumers will either toss it in the recycle bin or post to a forum like this rather than waste the trip to the store. Of the few that do, some will cuss and make a scene, a couple will post reviews—but at the end of the day the dealer looks at it as a numbers game. Unfortunate, and I'm glad I no longer work for a place that runs these.

TheRealMeatloaf, Comment to *I Just "Won" a 60" TV on a Scratch-Off Mass Mailer, What Am I In For*, REDDIT: R/ASKCARSALES (Apr. 17, 2018, 3:25 PM), https://reddit.com/r/askcarsales/comments/8cr8k2/i_just_won_a_60_tv_on_a_scratchoff_mass_mailer/dxj2xrr/ [https://perma.cc/SZC9-ERJ8].

118. *E.g.*, Yarrow, *supra* note 113.

119. *E.g.*, Marilyn Lewis, *10 Types of People Who Fall for Scams, Schemes and Cons*, MONEYTALKSNEWS (Oct. 17, 2017), https://www.moneytalksnews.com/10-types-people-who-fall-for-scams-schemes-and-cons/ [https://perma.cc/YJ9N-UUCS].

victimization because they were more exposed to predatory behavior the more time they spent online.[120] And so forth—there's no shortage of vulnerabilities scammers can use to extract money from their victims, or clever scammers looking for ways to do so.

3. Legal and Illegal Scams. Although many scams violate the law, there are enough that are legal, or that are not clearly illegal, that existing law is not a reliable solution to the problem of targeted scams. Many scams violate existing laws against fraud; many others amount to deceptive or unfair trade practices that violate the FTC Act. Some can amount to larceny or various other crimes or torts. But some scams don't fall into these buckets, and it's not clear that they ever could.

There are many reasons a scam might not violate the law. Sometimes there are simply gaps in the law, whether due to failure to anticipate a scam or due to the structure of a regulatory scheme. Election scams like the "Dinner with Trump" scam are a good example of the latter. Federal law sets out the requirements for a political action committee to operate, which include registering with the Federal Election Commission, disclosing the names of donors who give more than $200 in a calendar year, reporting how the committee spends its money, and filing periodic reports with the FEC.[121] Notably, federal law also governs the contents of fundraising solicitations, requiring that they contain specific disclaimers about who is soliciting money, how it will be used, and who paid for the solicitation.[122] Those requirements, however, serve different goals than laws like the FTC Act or criminal fraud law, seeking to further transparency and encourage political participation, while keeping a distance between campaigns and independent committees.[123] This means that while a fundraising solicitation might be deceptive or unfair by the standards of the FTC Act, it might be fine as a matter of federal election law so long as the fundraiser filed all the necessary FEC paperwork and made the proper disclosures. Indeed, in 2014, the FEC concluded that it should take no action against a PAC quite

120. Catherine D. Marcum et al., *Potential Factors of Online Victimization of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory*, 31 DEVIANT BEHAV. 381, 395–98 (2010).

121. *See* 52 U.S.C. §§ 30102(c), 30103(a), 30104 (Supp. V 2018); 11 C.F.R. §§ 100.1–116.11, 300.1–300.72, 9001.1–9039.3 (2019); FED. ELECTION COMM'N, CAMPAIGN GUIDE: NONCONNECTED COMMITTEES 3, 41–42, 47 (2008), http://www.fec.gov/pdf/nongui.pdf [https://perma.cc/9MXK-FTXS].

122. *See* 52 U.S.C. § 30120(a); 11 C.F.R. § 110.11.

123. *See, e.g.*, McConnell v. FEC, 540 U.S. 93, 120–32 (2003); Buckley v. Valeo, 424 U.S. 1, 66–68 (1976) (per curiam).

similar to American Horizons—this time the plot centered around Congressional candidate Allen West—because it concluded that the conduct was not "a fraud within the reach of the [Federal Election Campaign] Act or Commission regulation."[124] This is not an isolated incident; scammers have shifted from running scam charities to running scam political committees because they're less heavily regulated.[125]

Gaps like the one between election law and other anti-fraud and consumer-protection laws can be closed, whether through legislation, changes in judicial interpretation, or changes in agency interpretation or priorities. Indeed, in rejecting the West campaign's complaint, the FEC was careful to note that whether the PAC's activities were "prohibited by laws beyond the Act, criminal or otherwise, [was] not a matter within the Commission's jurisdiction."[126] The Federal Trade Commission recently started stepping in, going after companies that provide campaign services.[127] Even if the campaigns themselves are likely not

---

124. Factual and Legal Analysis at 1–2, Republican Majority Campaign PAC, MUR 6633 (F.E.C. Mar. 7, 2014), https://www.fec.gov/files/legal/murs/6633/14044352160.pdf [https://perma.cc/DFY6-FG72]. In that case, the PAC raised money with fundraisers saying things like "[i]t's up to us to Save Allen West" and "[h]elp Allen West win over the thousands of voters in his new Congressional district who have only been exposed to what they have heard in the media, and from his detractors. It's time for us to give them the truth about Allen West." *Id.* But the PAC spent almost nothing to help West's campaign. Complaint at 1, 3, Republican Majority Campaign PAC, MUR 6633 (F.E.C. Aug. 23, 2012), https://www.fec.gov/files/legal/murs/6633/14044352110.pdf [https://perma.cc/E7M4-5LHA]. The FEC observed that "[t]he record leaves little doubt that the [PAC] sought to use Representative West's likeness to raise funds independently to support his candidacy" and "it appears that the [PAC] spent very little of the money it raised to support West." It nevertheless concluded that the fundraiser didn't violate election law. Factual and Legal Analysis, *supra*.

125. *See* Maggie Severns & Scott Bland, '*Scam PACs' Rake in Millions Under Guise of Charity*, POLITICO (May 4, 2018, 5:04 AM), https://www.politico.com/story/2018/05/04/scam-pacs-political-action-committees-charity-investigation-568491 [https://perma.cc/4KJH-JR66] ("A POLITICO investigation finds operators under scrutiny for suspicious charity practices moving into politics, where election regulators have little power over them."). In addition to the different goals of federal election and consumer-protection law, charities are also more susceptible to regulation and enforcement actions because there are more regulators; states routinely regulate charities while playing little or no role in regulating federal elections. *See, e.g.*, Press Release, FTC, FTC Announces Operation False Charity Law Enforcement Sweep (May 20, 2009), https://www.ftc.gov/news-events/press-releases/2009/05/ftc-announces-operation-false-charity-law-enforcement-sweep [https://perma.cc/HA6J-ARTZ].

126. Factual and Legal Analysis, *supra* note 124, at 1.

127. *See, e.g.*, Complaint at 4–5, United States v. InfoCision, Inc., No. 5:18-cv-00064 (N.D. Ohio Jan. 10, 2018) (settling with a telemarketing firm that allegedly violated the Telemarketing Sales Rule); Maggie Severns & Derek Willis, *How Conservative Operatives Steered Millions in PAC Donations to Themselves*, POLITICO (July 26, 2019, 5:04 AM), https://www.politico.com/story/2019/07/26/conservative-majority-fund-political-fundraising-pac-kelley-rogers-1428260 [https://perma.cc/86WV-94V6] (discussing how InfoCision

"commerce" within the meaning of the FTC Act, the campaign process is still subject to some FTC regulation.

These gaps can be hard or impossible to close. Sometimes this is because a regulatory scheme legitimately prioritizes different goals than avoiding scams. The caller-ID system is a good example. When a telephone call is placed, the phone company serving the recipient pays a fraction of a penny to look up the caller's name in a caller-ID database. Scammers have exploited this fact by colluding with database providers to make money from millions of robocalls.[128] When recipients look up the dialer's number (or forged number), the database provider collects a fraction of a penny and kicks some of that back to the number's owner. This means that the caller makes money even if no one ever answers the calls because the payment comes when the recipient phone company performs an automatic database lookup while connecting the call. Because reliable universal service is the overriding goal of the phone system, though, phone companies have been reluctant to try to filter out these robocalls.[129]

Other times, regulatory gaps and loopholes aren't closed because the political process makes it impossible to do so, even if there is little good reason. The dietary-supplement industry in the United States is a good example. Vitamins, minerals, herbs, amino acids, and other dietary supplements are a $37 billion industry in the United States, even though most of those products haven't been shown to provide any benefit at all, and even though some of them can be actively harmful.[130] Under the Dietary Supplement Health and Education Act, sellers can make claims like "great for joint health!" so long as they include a disclaimer saying "This

provided services to political committees and the FTC's responsive actions).

128. *See, e.g.*, Complaint at 5–6, FTC v. Caribbean Cruise Line, Inc., No. 0:15-cv-60423 (S.D. Fla. Mar. 3, 2015); Sarah Krouse, *Why Robocallers Win Even if You Don't Answer*, WALL ST. J. (June 4, 2018, 5:30 AM), https://www.wsj.com/articles/why-robocallers-win-even-if-you-dont-answer-1528104600 [https://perma.cc/YXX5-Z28K]; John D. McKinnon, *FCC Fines Man $120 Million for His 100 Million Robocalls*, WALL ST. J. (June 22, 2017, 6:18 PM), https://www.wsj.com/articles/fcc-proposes-120-million-fine-against-miami-telemarketer-1498152920 [https://perma.cc/LLV7-6FYJ].

129. Merrit Kennedy, *FCC Wants Phone Companies to Start Blocking Robocalls By Default*, NPR (May 15, 2019, 7:14 PM), https://www.npr.org/2019/05/15/723569324/fcc-wants-phone-companies-to-start-blocking-robocalls-by-default [https://perma.cc/59GT-HM6X]; *see also* CONSUMER & GOV'T AFFAIRS BUREAU, FED. COMMC'NS COMM'N, CG DOCKET NO. 17-59, REPORT ON ROBOCALLS 7 & n.33 (2019), https://docs.fcc.gov/public/attachments/DOC-356196A1.pdf [https://perma.cc/P7YY-H4WV] (discussing the Commission's prior reluctance to allow call blocking).

130. *See, e.g.*, Erin Brodwin, *The $37 Billion Supplement Industry Is Barely Regulated—and It's Allowing Dangerous Products to Slip Through the Cracks*, BUS. INSIDER (Nov. 8, 2017, 2:58 PM), https://www.businessinsider.com/supplements-vitamins-bad-or-good-health-2017-8 [https://perma.cc/8KCE-4MRR].

statement has not been evaluated by the Food and Drug Administration. This product is not intended to diagnose, treat, cure, or prevent any disease."[131] The Act, which effectively deregulated health claims made by supplement manufacturers, was a public-choice triumph, with a powerful industry successfully overcoming strenuous objections from the Food and Drug Administration and essentially legalizing scam supplements.[132]

Scams that depend on violating consumer expectations, not express representations, likewise might be legally fine, or hard for agencies or law-enforcement officials to pursue. Another common telephone scam, for instance, works because the telephone country code for the United States, +1, also covers Canada and most Caribbean nations. A phone number from one of those nations looks to an American like a domestic phone number in an unfamiliar area code like 242 (the Bahamas), 649 (the Turks and Caicos), or 784 (Saint Vincent and the Grenadines). A customer, then, who misses a call that appears to come from a random domestic number, and calls it back, may actually be calling a foreign country. Calls to foreign nations are, of course, not domestic calls, and can be far more expensive than customers expect. A scammer can exploit this misunderstanding by setting up an auto-dialer in a foreign country (or domestically, using forged caller-ID info) that charges high fees for inbound calls; calling random American telephone numbers and hanging up before anyone answers; waiting for callers to return the calls; and trying to keep those callers on the phone for as long as possible, collecting charges on the order of several dollars per minute for calls that callers expect to be free.[133] Exploiting this kind of misunderstanding or expectations mismatch is the basis for lots of scams, and much of the time there's nothing illegal about it.[134]

---

131. Dietary Supplement Health and Education Act of 1994, Pub. L. No. 103-417, § 6, 108 Stat. 4325, 4329 (1994) (codified as amended at 21 U.S.C. § 343(r)(6) (2012)).

132. *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-662T, HERBAL DIETARY SUPPLEMENTS: EXAMPLES OF DECEPTIVE OR QUESTIONABLE MARKETING PRACTICES AND POTENTIALLY DANGEROUS ADVICE 1, 13–14 (2010) (testimony of Gregory D. Kutz, Managing Director, Forensic Audits and Special Investigations); Margaret Gilhooley, *Deregulation and the Administrative Role: Looking at Dietary Supplements*, 62 MONT. L. REV. 85, 93–95 (2001); Arlene Weintraub, *Dietary Supplements: Latest Government Uproar No Match for Industry Lobbying Money*, CBS NEWS (June 1, 2010, 4:30 PM), https://www.cbsnews.com/news/dietary-supplements-latest-government-uproar-no-match-for-industry-lobbying-money/ [https://perma.cc/C234-STKF].

133. *E.g.*, Kristin Wong, *Phone Calls from These Area Codes Might Be a Scam*, LIFEHACKER (Mar. 10, 2017, 1:30 PM), https://lifehacker.com/phone-calls-from-these-area-codes-might-be-a-scam-1793107601 [https://perma.cc/YYC3-QHSL].

134. One more example, just for fun. Murano glass is a term that technically includes hand-blown glass made on the Italian island of Murano, just outside Venice. It's often used,

The bottom line, then, is that laws against scams might inevitably be an incomplete solution. Even when those problems can be overcome and laws can be well tailored to address scams, they may nevertheless fail to address the problem because targeting itself can make it easier to scam people, as discussed in the next Section.

B. How Targeting Platforms Facilitate Scams

Just as the combination of more data and better targeting made advertising more efficient, it also made it easier and more efficient for scammers to scam people.

No one theory explains when and why scams occur, but criminologists have developed numerous helpful approaches. One of those theories, routine activity theory, provides a positive model of the ways that changes to an environment affect the rate of criminal activity. (Though not all scams are crimes, the theory nevertheless provides a useful lens for looking at scams because the effects of environmental changes should be similar for the two overlapping categories.) Routine activity theory suggests that three things must converge for a crime to occur: a motivated offender, a suitable target, and the absence of a "capable guardian[]" to prevent the crime.[135] When something changes and these convergences happen more often, the amount of crime can be expected to rise. For instance, if social patterns change such that people stay home less often and go out to dinner more often, the number of home burglaries might rise in response, because the

though, to refer to certain styles of glass, so lots of shops in Murano and elsewhere in Italy sell glassware and art that looks like Murano glass and carries prominent "made in Italy" stickers. Sometimes these stickers are lies and a piece has been mass-produced elsewhere, but sometimes an item is made in Italy—just not on Murano, which matters to collectors. When a piece actually is made in Italy, such a sticker seeks to capitalize on the mismatch between consumers' understanding or expectations—the assumption that something made in Italy is real Murano glass—and the legally required disclosure, which just reports the country of origin. To fight back against this scam, genuine Murano glassmakers have developed a distinctive logo and educational campaign, with real pieces labeled with a sticker containing the logo and a data-matrix code leading to a website providing information about the piece and its maker. By working to realign consumers' expectations with reality, the genuine Murano glassmakers reduce the effectiveness of the scam, or at least divide the market so that savvy shoppers willing to pay for the real thing can do so without fear. *See, e.g.*, *Guide*, MURANO GLASS, http://www.muranoglass.com/en/guide/ [https://perma.cc/RC2W-XFKU] (last visited Sept. 12, 2019); Chiara Vasarri, *Venice Glassmakers' Ancient Art Shattered by Slump, Taxes*, BLOOMBERG BUSINESSWEEK (Dec. 1, 2014), https://www.bloomberg.com/news/articles/2014-12-01/venice-glassmakers-ancient-art-shattered-by-weak-demand-taxes [https://perma.cc/Y8Z5-S4RF].

135. Routine activity theory was originally described in Lawrence E. Cohen & Marcus Felson, *Social Change and Crime Rate Trends: A Routine Activities Approach*, 44 AM. SOC. REV. 588, 589–90 (1979).

three factors that must converge for a home burglary to occur will come together more often. The theory provides useful predictions about changes in the rates of certain crimes, especially ones characterized by their opportunistic or predatory natures.[136]

Targeting makes it easier to scam people online because it makes it easier for these convergences to occur and for scams to succeed when they do occur. It does this by making three things easier for scammers: targeting their victims, hiding from platforms and law enforcement, and developing better and more-effective scams in the first place.

1. Better Targeting. Just as with advertising, better targeting helps scammers because it makes it easier to reach potential victims, the intended consumers of the scam. Targeting doesn't necessarily do this by increasing the number of times that a motivated scammer, suitable target, and lack of a capable guardian converge; if scammers showed their ads to everyone instead of targeting certain victims, then they would undoubtedly find some victims who would not have been obvious targets. But just as targeting makes advertising cheaper and more efficient, it makes it cheaper and more efficient for a scammer to reach the best potential victims. In the long run, this should result in more scammers taking advantage of more victims, because some additional scammers will enter the market when running a scam is cheaper, while other scammers will get a better return on their investment—target more promising victims—for a fixed budget.

The key difference between targeted advertising and targeted scams is that targeting is useful for scammers in ways it isn't for ordinary advertisers. To be sure, targeting is useful for scammers for all the same reasons that apply to advertising. As discussed before, with advertising, the usual goal of targeting is to choose the demographics and other characteristics that reflect a consumer's likelihood of buying an advertised product or service.[137] Rolex targets wealthy consumers; government contractors target government employees; and so on. With better

136. Cohen and Felson discuss several empirical findings consistent with the theory. *Id.* at 594–604. The theory has since been tested in numerous studies. *See generally* Fawn T. Ngo & Raymond Paternoster, *Cybercrime Victimization: An Examination of Individual and Situational Level Factors*, 5 INT'L J. CYBER CRIMINOLOGY 773, 774–76 (2011) (citing studies); *see also* TERANCE D. MIETHE & ROBERT F. MEIER, CRIME AND ITS SOCIAL CONTEXT: TOWARD AN INTEGRATED THEORY OF OFFENDERS, VICTIMS, AND SITUATIONS 1–8 (Ronald A. Farrell ed., 1994) (arguing that integrated theories that account for offenders' decisions to engage in crime and victims' behaviors that increase their vulnerability to crime provide a better account of crime levels than individual theories of criminality and victimization).

137. *See supra* Section II.B.

targeting, this can be improved—instead of all wealthy consumers, Rolex might target those who have looked at the Rolex website or read reviews of nice watches, or whose behavior indicates a psychological tendency toward flashy goods like luxury watches, or a trusting nature that might be easy to take advantage of[138]—but the goal is still to target the consumers who are likely to be interested in buying the advertised product. This form of targeting works equally well for scams because scammers want to find the consumers who would be interested in a scam, just like any advertiser would. A scam purporting to offer investment opportunities or manage household wealth might target wealthy retirees, while a scam purporting to help first-time homebuyers might target younger victims.[139] The goal is the same: to choose the consumers most likely to respond to the message.

There are other reasons targeting is useful for scammers. For one, scammers can use targeting to find the victims whose *vulnerabilities* make them likely to fall for a scam—something that's usually not the goal in ordinary advertising. All scams prey on vulnerabilities of one kind or another; sometimes it's as simple as creating a sense of urgency so the victim acts now instead of carefully considering the offer and discussing it with others.[140] But there are other, more-specific vulnerabilities that scammers seek to exploit, and because these vulnerabilities aren't as universal as responding emotionally to urgency, they benefit from targeting to narrow the pool of potential victims.

---

138. *Cf.* Jillian J. Turanovic & Travis C. Pratt, *"Can't Stop, Won't Stop": Self-Control, Risky Lifestyles, and Repeat Victimization*, 30 J. QUANTITATIVE CRIMINOLOGY 29, 45–47 (2014) (finding that measures of self-control predict levels of repeat victimization, suggesting that online psychological profiles could be used to identify potential victims); Ngo & Paternoster, *supra* note 136, at 785–87 (finding a similar, but weaker, relationship in online victimization); Gustavo S. Mesch & Guy Beker, *Are Norms of Disclosure of Online and Offline Personal Information Associated with the Disclosure of Personal Information Online?*, 36 HUM. COMM. RES. 570, 587–89 (2010) (finding that norms of personal-information disclosure online and offline are only weakly related, suggesting that online disclosure would be a promising avenue for identifying potential victims); Gustavo S. Mesch, *Is Online Trust and Trust in Social Institutions Associated with Online Disclosure of Identifiable Information Online?*, 28 COMPUTERS IN HUM. BEHAV. 1471, 1476 (2012) (containing similar findings); Marcum et al., *supra* note 120, at 395–98 (containing similar findings).

139. *E.g.*, *Common Fraud Schemes: Investment Fraud*, FBI, https://www.fbi.gov/scams-and-safety/common-fraud-schemes/investment-fraud [https://perma.cc/3J8W-VRD5] (last visited Sept. 12, 2019); Stuart Ross & Russell G. Smith, *Risk Factors for Advance Fee Fraud Victimisation*, TRENDS & ISSUES CRIME & CRIM. JUST., Aug. 2011, at 1, 4–5, https://aic.gov.au/publications/tandi/tandi420 [https://perma.cc/TE2B-Z3GR].

140. *E.g.*, Yarrow, *supra* note 113 (observing that "the standard fraud playbook is to create a sense of urgency, which elevates emotions and decreases rationality").

Useful vulnerabilities could include any of a variety of characteristics, depending on the scam; just as different kinds of scams victimize different kinds of people, different kinds of scams might rely on different kinds of online targeting to find different kinds of vulnerabilities. A scammer pitching a fraudulent subprime-mortgage or debt-consolidation scam, for instance, might target consumers who are poor, in significant debt, or in bankruptcy, or those who search Google for information about payday lenders or visit their websites. These scams capitalize on financial desperation, which can cause people to seek implausible fixes if the obvious ones haven't worked.[141] Or, a scammer offering get-rich-quick investment schemes might look for retirees with substantial savings, capitalizing on vulnerabilities like cognitive decline or loneliness.[142] Or such a scammer might look for people who trade individual stocks and make a lot of trades, suggesting that they become bored and are willing to change up their investments looking for higher returns.[143] A scam selling a

141. Three FTC surveys of consumer fraud conducted between 2004 and 2011, for instance, found that consumers with incomes less than $40,000 were more likely to fall for scams than those with higher incomes. *See* KEITH B. ANDERSON, FED. TRADE COMM'N, CONSUMER FRAUD IN THE UNITED STATES: AN FTC SURVEY 59 (2004) [hereinafter ANDERSON, AN FTC SURVEY]; KEITH B. ANDERSON, FED. TRADE COMM'N, CONSUMER FRAUD IN THE UNITED STATES: THE SECOND FTC SURVEY 28 (2007) [hereinafter ANDERSON, THE SECOND FTC SURVEY]; KEITH B. ANDERSON, FED. TRADE COMM'N, CONSUMER FRAUD IN THE UNITED STATES, 2011: THE THIRD FTC SURVEY 50 (2013) [hereinafter ANDERSON, THE THIRD FTC SURVEY].

142. For a useful overview of financial exploitation of the elderly, see Marguerite DeLiema & Kendon J. Conrad, *Financial Exploitation of Older Adults*, *in* ELDER ABUSE: RESEARCH, PRACTICE AND POLICY 141 (XinQi Dong ed., 2017). DeLiema and Conrad review several competing explanations for why scammers would target the elderly, including declining health, isolation and undue influence, and increased opportunity for exploitation. *Id*. at 143–46. Though each of these theories has some support, they have strikingly different consequences. Notably, the evidence does not always back up the intuition that elderly people are more likely to fall for scams; rather than being unusually vulnerable to scams, they may simply be targeted more often, though it's hard to know for certain because reporting rates are low. *See id.* at 144–45; Richard M. Titus et al., *Victimization of Persons by Fraud*, 41 CRIME & DELINQ. 54, 60–62 (1995); ANDERSON, AN FTC SURVEY, *supra* note 141, at 68 ("Perhaps the most noteworthy finding here is that consumers aged 65 or over do not appear to be at greater risk of being a victim than those who are somewhat younger. Indeed, the cross-tab results suggest that seniors face the lowest risk of being a victim."); ANDERSON, THE SECOND FTC SURVEY, *supra* note 141, at 40; ANDERSON, THE THIRD FTC SURVEY, *supra* note 141, at 97–98.

143. *Cf.* Kristy Holtfreter et al., *Low Self-Control, Routine Activities, and Fraud Victimization*, 46 CRIMINOLOGY 189, 206–09 (2008) (finding no evidence that those with weak self-control were more likely to be targeted, but that those who more frequently were in situations where they could be targeted were indeed targeted more often); Gustavo S. Mesch & Matias Dodel, *Low Self-Control, Information Disclosure, and the Risk of Online Fraud*, 62 AM. BEHAV. SCIENTIST 1356, 1366 (2018) (finding weak evidence that "[i]ndividuals who indicate that they are willing to take risks on financial investments or have accumulated more debt than they can handle are more likely to be targets" of scams).

worthless cure might target people who search for information about a particular disease, targeting a different kind of desperation. Each of these targets a particular vulnerability that only some people will have: poverty or desperation for a cure, or a tolerance for risk and lack of self-control that leads one to disregard conventional investment wisdom to find higher returns. Whatever vulnerability a scammer seeks to exploit, targeting tools make it much easier to identify individuals with that vulnerability.

In one sense, this is no different than any other targeted advertising. Both ordinary targeted advertising and targeted scams look for the audiences that are believed to be most likely to respond to the ad. There is a difference, though: while advertisers ordinarily target demographics and characteristics that indicate consumers who are likely to be interested in the advertised products—in the usual case, presumably because they want that product—scammers might instead choose demographics and characteristics that indicate people who are predisposed to fall for a particular scam. No one wants to fall for a scam, though; that's part of what makes it a scam.[144] This is essentially, then, a special case of the general point about targeting groups with specific demographics or other characteristics; the difference is that there's no argument that targeting vulnerable victims has any social value.

Another reason that targeting is useful for scammers is that they can use targeting to find victims with *specific beliefs* instead of specific vulnerabilities. This is another variant on targeting groups with specific characteristics, but it opens new avenues of persuasion for scammers. The "Dinner with Trump" scam is an obvious example: by targeting individuals who supported Trump's candidacy, the American Horizons PAC had an audience that wanted to support the purported mission of the scam.[145] Likewise, scams might target individuals with specific political, religious, or

144. I set aside the case of someone who wants to fall for a scam, or is willing to do so, for entertainment value or out of loneliness or out of a general taste for chaos. In those cases, arguably the scam isn't a scam at all, because it's providing the victim some utility, even if it's not the utility the scammer purports to provide.

145. Politico reported, for instance, that every donor it reached who had given money to American Horizons thought he or she was giving to the Trump campaign. Goldmacher, *supra* note 1. One donor, contacted by Politico, said, "I feel ripped off and taken advantage of. This is horrible. [Giving to an independent PAC] was not my intent." She added, "I want my money back and I want them to add up what they stole from people and give it to Donald Trump." *Id.* Another donor explained, "I had planned to give a thousand bucks to his campaign, and when my wife saw it also on her Facebook feed she said, 'Why not do this?'" *Id.*

moral beliefs, and tailor the content of the scam to appeal to victims with those beliefs.[146] This is a long-time technique used by scammers. Indeed, the FBI warns that investment schemes "often seek to victimize affinity groups—such as groups with a common religion or ethnicity—to utilize the common interests to build trust to effectively operate the investment fraud against them."[147]

This kind of targeting has a few effects. One effect is that it selects for individuals likely to respond to the scam; in this sense, it is just like normal targeted advertising, which seeks to avoid wasting money on people who don't want the advertised product. Another is that it also makes the viewer more likely to fall for the scam. A substantial body of psychological research demonstrates that people are more likely to believe information that conforms to their ideological priors, even if it is illogical, internally contradictory, or unsupported by evidence.[148] A scammer who reinforces those priors, then, can take in victims who otherwise wouldn't fall for the scam.

The result of all these forms of targeting is that scammers, just like advertisers in general, can more efficiently reach the individuals they want to reach without wasting money on individuals who are less likely to pay off. While economic theory offers a basis for thinking this efficiency might be socially valuable in the case of advertising,[149] these arguments don't translate to scams. Scams are a poor fit for the information theory of advertising, almost by definition, because scams don't work when victims have full information and because victims don't benefit from falling for scams. Better information will just make the scam harder to pull off.[150] Scams are a much better fit for the persuasion theory of advertising, with a scammer seeking to shape demand

---

146. The nutritional-supplement industry—discussed above, *see supra* notes 130–32 and accompanying text—provides an especially striking example of how appeals can be tailored to different groups of potential victims. For instance, both Alex Jones's Infowars and Gwyneth Paltrow's Goop sell basically the same, largely worthless powders and pills to very different audiences using very different branding and marketing. Nikhil Sonnad, *All the "Wellness" Products Americans Love to Buy Are Sold on Both Infowars and Goop*, QUARTZ (June 29, 2017), https://qz.com/1010684/all-the-wellness-products-american-love-to-buy-are-sold-on-both-infowars-and-goop/ [https://perma.cc/4U8V-EPDB]. Powders and pills aren't their only scams. *See, e.g.*, Rae Paoletta, *NASA Calls Bullshit on Goop's $120 'Bio-Frequency Healing' Sticker Packs [Updated]*, GIZMODO (June 22, 2017, 9:20 AM), https://gizmodo.com/nasa-calls-bullshit-on-goops-120-bio-frequency-healing-1796309360 [https://perma.cc/VZ6K-TS69].

147. *Common Fraud Schemes: Investment Fraud*, *supra* note 139.

148. *E.g.*, Daniel M. T. Fessler et al., *Political Orientation Predicts Credulity Regarding Putative Hazards*, 28 PSYCHOL. SCI. 651, 657–59 (2017); *see also infra* note 156.

149. *See supra* Section II.A.

150. *See supra* Section III.A.1.

by persuading victims that a bad opportunity is in fact a good one; if the opportunity were good, it wouldn't be a scam. Even though advertising theory can paint an optimistic or a pessimistic portrait of targeted advertising, with targeted scams only the pessimistic version is plausible.

There is a significant objection to this reasoning, albeit an unappetizing one. A scam might make its victim worse off, but it does not follow that the scam itself is harmful; if it benefits the scammer more than it harms the victim, then the scam might be welfare-enhancing on the whole. This might occur, for instance, if the scammer had a greater marginal utility of money than the victim. Just as a starving thief stealing bread might increase social welfare, a needier scammer taking from less-needy victims might, overall, be a good thing.[151] Such a scenario is unlikely to occur, though, for at least two reasons. First, if a scam were to generate more surplus for the scammer than it costs the victim, then the scammer could simply pay the victim the difference and the transaction would no longer be a scam. The transaction costs between scammer and victim should, in most cases, be small, so when this doesn't happen it suggests that the scam is probably not welfare-enhancing. Second, the welfare consequences of a hypothetical welfare-enhancing scam would need to consider changes to potential victims' incentives and behavior, which could be substantial. If, for example, people had to protect themselves from scams, then those costs—which are pure waste—might dwarf the net benefits to scammers because the universe of potential victims is large.[152] Or, if potential victims forego opportunities or experiences to avoid being scammed, then those lost opportunities might outweigh any benefits to scammers.[153]

The upshot, then, is that targeting makes scams more efficient, and more-efficient scams are very likely to hurt society. By compiling and productizing detailed profiles of individual

---

151. *Cf. Proverbs* 6:30 ("People do not despise a thief if he steals to satisfy his hunger when he is starving."); VICTOR HUGO, LES MISÉRABLES 51–52 (Frederick Mynon Cooper ed., 1862).

152. *See, e.g.*, Angelo Antoci et al., *Self-Protection, Psychological Externalities, and the Social Dynamics of Fear*, 61 J. CONFLICT RESOL. 349, 351–53 (2017); Ann P. Bartel, *An Analysis of Firm Demand for Protection Against Crime*, 4 J. LEGAL STUD. 443, 478 (1975) (discussing firm expenditures for protective measures); Isaac Ehrlich, *Crime, Punishment, and the Market for Offenses*, J. ECON. PERSP., Winter 1996, at 43, 48–51; Isaac Ehrlich & Gary S. Becker, *Market Insurance, Self-Insurance, and Self-Protection*, 80 J. POL. ECON. 623, 640 (1972).

153. *See, e.g.*, W. David Allen, *Self-Protection Against Crime Victimization: Theory and Evidence from University Campuses*, 32 INT'L REV. L. & ECON. 21, 32 (2013) ("'[I]ndividuals desire protection from crime, but protection comes at a cost,' and sometimes that cost takes the form of foregone opportunities to enjoy social activity.").

users, the Facebooks and Googles of the world—along with literally thousands of tracking companies most people have never heard of—make it easier for the Ian Haweses of the world to set up new scams.

2. Better Hiding. In addition to making it easier for scammers to target victims, data platforms like Facebook also make it easier for them to evade detection by law-enforcement officials and other authorities. These authority figures can play two distinct roles when it comes to scams. In one role, the simple presence of an authority figure can prevent a scam from operating, much like the presence of a guard in a store might prevent a robbery. In this role, better hiding changes the incidence of scams by directly affecting one of the three things that must come together for a scam to happen: the lack of a capable guardian. In the other role, authority figures operating after-the-fact to detect, prevent, and remediate scams—working more like detectives than in-store security guards. This is less direct, shutting down motivated scammers rather than preventing individual scams from occurring. But it probably has a greater effect in the long run.

Targeting doesn't really affect the first role of authority figures because that kind of authority mostly doesn't exist for online transactions. With narrow exceptions—certain bank and investment transactions, for instance—online transactions don't generally have to be approved or monitored by any authority figure before they happen. If someone gives money to the American Horizons PAC or buys a worthless Super Male Vitality supplement, the transaction happens without an opportunity for a capable guardian to step in.[154] It matters very much, though, if authority figures detect and shut down scams, because a scam that operates for less time can ensnare fewer victims and because a scam that is expected to ensnare fewer victims will appeal to fewer scammers.

Targeting does affect the second role, however, making it harder for authorities to detect scams by affecting each of the ways that authorities might do so in the first place. There are three basic means by which authorities can detect scams: reports by victims and intended victims, reports by witnesses, and investigation by the authorities themselves. Targeting makes each of these

154. Though, online (and offline) stores increasingly use algorithms to block transactions that they conclude have a high likelihood of being fraudulent. *E.g.*, Khadeeja Safdar, *Why Paying for Fast Shipping Could Get You Flagged as a Fraudster*, WALL ST. J. (Apr. 19, 2018, 10:07 AM), https://www.wsj.com/articles/why-paying-for-fast-shipping-could-get-you-flagged-as-a-fraudster-1524139200 [https://perma.cc/SA4Y-KLAH]. For more on fraud-detection algorithms, see *infra* Section IV.A.

mechanisms less likely to work, whether the authorities are law-enforcement officials, journalists, public-interest groups, or other third parties. This Section explains how targeting makes it easier for scammers to evade detection through these three means.

Reports by Victims and Intended Victims. The easiest way to detect a scam may be to wait for a victim, or intended victim who doesn't fall for the scam, to report it once it happens. Someone who gives money to a scam PAC, and later learns the truth, might report the PAC to the Federal Election Commission or to a campaign or reporter; someone who dials an expensive overseas number in response to a Caller ID scam might see the bill and report the scam to her phone company.

Waiting for victims to report scams is a low-cost method of detection because it requires little up-front investment—essentially just setting up some way to process incoming reports. It can, however, be an inefficient means of detection when victims and intended victims are unlikely to report a given scam because a scammer could victimize many people before law-enforcement officials learn of the scam's existence. The likelihood that someone will report a scam, therefore, matters greatly: if victims and intended victims are likely to do so, then the scam can quickly be shut down, but if they are unlikely to report a scam, then many people could fall victim before someone takes the steps necessary to report the scam. And this is a real problem because many scams are under-reported.[155]

Targeting makes it less likely that victims and intended victims will report a scam, for two major reasons. Targeting can reduce the number of people exposed to a scam, even while keeping constant the size of the scam or the amount of money it makes, because it reduces the number of uninterested people who are exposed to it. It can also change who sees the scam, causing it to be seen by the potential victims who are least likely to believe it's a scam. This lets scammers take advantage of their potential victims' motivated reasoning, which tends to distort people's thinking in favor of their preferred outcomes.[156] As mentioned above, this means that they are more likely to fall for it, but it also means that they are less likely to report it. A get-rich-quick scam

155. *See supra* Section III.A.2.

156. *See, e.g.*, Kari Edwards & Edward E. Smith, *A Disconfirmation Bias in the Evaluation of Arguments*, 71 J. PERSONALITY & SOC. PSYCHOL. 5, 18–22 (1996); Ziva Kunda, *The Case for Motivated Reasoning*, 108 PSYCHOL. BULL. 480, 493–95 (1990); David P. Redlawsk et al., *The Affective Tipping Point: Do Motivated Reasoners Ever "Get It"?*, 31 POL. PSYCHOL. 563, 564 (2010); Drew Westen et al., *Neural Bases of Motivated Reasoning: An fMRI Study of Emotional Constraints on Partisan Political Judgment in the 2004 U.S. Presidential Election*, 18 J. COGNITIVE NEUROSCIENCE 1947, 1955 (2006).

that targets people who want to become rich, or a fake cure that targets people with an incurable disease, has an audience that wants the scam to be true, and so will do the cognitive work to believe it is true, all evidence to the contrary. This works best when the viewer has an emotional stake in the issue—which is precisely what scammers try to take advantage of.

The net effect, then, is that a targeted scam can be seen by fewer people, and those that do see it can be more likely to believe it and less likely to report it to authorities. The overall chances, then, that anyone reports the scam can be much lower than they would be for the same scam without targeting. Yet the scam can make just as much money—or more—targeting a smaller audience.

Reports by Witnesses. Witnesses who are not victims can also report scams to authorities. Targeting should make it less likely that a witness will report a scam, for many of the same reasons as apply to victims and potential victims: there will be fewer witnesses to a scam, and those witnesses who do exist may be less likely to report.

The first point is straightforward. Witnesses can learn of a scam in many ways, but the number of potential witnesses will depend on how many potential victims the scammer targets, because the more widely distributed information is about a scam the more people will encounter that information. When a scammer can target fewer people, there will be fewer potential witnesses.

The second point is subtler. Witnesses might be more likely or less likely than victims to report scams. Unlike victims, they have nothing at stake, and so may not care enough to report them, but they may also be less likely to avoid reporting due to motivated reasoning or embarrassment. Different witnesses, though, likely have different propensities to report scams, and in addition to changing the number of potential witnesses, targeting changes the kinds of people who might become witnesses. While witnesses might be *less* affected by motivated reasoning than a scam's victims would be, they might still be affected. Because targeting will tend to select similar people, there should often be similarities between victims and witnesses. Many of the potential witnesses of the American Horizons scam, for instance, are themselves likely to be Trump supporters, because those are the people the ads targeted and also the people most likely to know and associate with the victims of the scam; likewise with scams targeting the poor, the elderly, specific religious groups, immigrant populations, and so forth. If witnesses share characteristics that cause victims to believe a scammer, then the witnesses might likewise be credulous of the scam and so less likely to report it.

Independent Investigation. Even without a report from a victim or witness, law-enforcement agencies and others can uncover scams through their own independent investigation. Many of these investigators will be government employees, including those working in police departments or prosecutors' offices or for agencies like the Federal Trade Commission, Securities and Exchange Commission, or offices of state attorneys general. Others could be journalists, nonprofit consumer-protection groups, academics, activists, or other interested outsiders. Though most scams that come to investigators' attention are likely reported, investigators can also uncover them on their own. For instance, an agency might randomly send undercover investigators into businesses to see if they act honestly;[157] or it might perform statistical analyses on reported data to detect patterns indicative of fraud.[158]

Targeting hinders this form of detection as well, because investigators are more likely to come across a scam when information about that scam is exposed to the public, but targeting minimizes the amount of information so exposed. Keeping scams hidden has often been a goal of scammers, but doing so can run counter to the need to attract victims. Targeting lets a scammer have it both ways: making the scam known to potential victims while keeping it hidden from others. This isn't new—a scammer who pitches retirees on an investment scheme would be dumb to pitch those who don't fit the profile—but online targeting automates this filtering process and lets it happen at scale.

Authorities might come across scams anyway, but targeting means they're much less likely to do so on their own. Most investigators aren't likely to be members of the groups targeted by scammers, so they won't naturally see scam ads. They could instead try to fake it—the online equivalent of undercover work—but doing so is unlikely to work without a lot of effort.

157. *See, e.g.*, Eric Lichtblau & William M. Arkin, *More Federal Agencies Are Using Undercover Operations*, N.Y. TIMES (Nov. 15, 2014), https://www.nytimes.com/2014/11/16/us/more-federal-agencies-are-using-undercover-operations.html [https://perma.cc/T3VY-SPSY].

158. The Securities and Exchange Commission, for instance, has an Analysis and Detection Center that analyzes market activity, looking for signs of illegal insider trading. *See* Reuters, *Here's How the SEC Is Using Big Data to Catch Insider Trading*, FORTUNE (Nov. 1, 2016), http://fortune.com/2016/11/01/sec-big-data-insider-trading/ [https://perma.cc/3AZ9-PM4E]. Similarly, there are mathematical techniques to detect fraudulent accounting results. Benford's Law, for instance, is the observation that the first digits of numbers in real-world data often follow a logarithmic distribution, with 1 appearing more often than 2, 2 more often than 3, and so forth. Financial data that fails to obey the law can be a sign of fraud. *See* Cindy Durtschi et al., *The Effective Use of Benford's Law to Assist in Detecting Fraud in Accounting Data*, 5 J. FORENSIC ACCT. 17, 19–22 (2004).

Investigators could, for example, set up dummy profiles fitting various groups that might be targeted by scammers. This requires a lot of foresight, though, to identify the right groups; before the American Horizons scam came to light, would many officials have identified Trump supporters as potential victims? Moreover, it would take a lot of work to maintain profiles for different potential targets because targeting can draw from many sources of information, like browsing history, retail transaction data, reading habits, consumer surveys, and more.[159] An investigator could take the easy route and just tell Google or Facebook that a dummy profile is a member of a targeted group, but if they don't take the time to engage in all the normal online activities that a real member of that group would, then even a mildly sophisticated tracking system won't target them alongside real potential victims. It's like sending an undercover cop into a school to find a drug dealer: the dealers will probably realize that something is up when the new kid doesn't act like a typical student.[160]

The net effect of targeting, then, should be to make it easier for scammers to hide their activities and harder and more expensive for authorities to detect them. This will matter to a different degree depending on the scam because different kinds of scams will require different kinds and amounts of detection. Some scams will be illegal and cause a lot of harm, so authorities will want to work hard to eliminate them and prosecute their perpetrators; others will cause less harm and so be lower priorities. With legal scams, policymakers might want to learn what scams exist so they can change the law to eliminate them, or they might conclude that the law should do nothing about a particular scam, leaving detection to interested outsiders like consumer-protection groups. Targeting should affect all these kinds of investigation, hindering all of these goals.

3. Better Scams. The third way that targeting platforms facilitate scams is by helping scammers develop and deploy better, more-effective scams. Rather than changing the number of times a motivated scammer, suitable target, and lack of a capable guardian coincide, this changes the likelihood that when these things come together, the scam will succeed. Targeting platforms help scammers develop better scams in two ways: by giving scammers the ability to quickly test and improve their scams and

159. *See supra* notes 54–62 and accompanying text.

160. *See, e.g.*, 22 JUMP STREET (Columbia Pictures & Metro-Goldwyn-Mayer Pictures 2014). *But see* 21 JUMP STREET (Columbia Pictures & Metro-Goldwyn-Mayer Pictures 2012).

by making it possible to run individualized versions of the scam tailored to individual victims.

Testing and Improving Scams. The main benefit that targeting platforms provide to advertisers is the ability to choose who sees an ad, but another benefit is increasingly important: the ability to figure out what that person should see in the first place. Targeting platforms provide this benefit by making it possible to test and compare hundreds or thousands of ads, or versions of an ad, quickly and at scale. Tracking and testing are, conceptually, unrelated services, but because both depend on many of the same underlying technological requirements (quickly serving different content to different users and recording those users' behavior and outcomes) and serve the same goals (optimizing ad performance), the two are often offered together or are designed to work together.[161]

Testing different ads to figure out what works best is something that advertisers have always sought to do, but the tools available for doing so have historically been limited by technology because most ads can't be customized for individual readers and viewers. To test a tv or magazine campaign, a company's best options have usually been tools like focus groups or test marketing—running different ad campaigns in Minneapolis and Milwaukee, for instance, and seeing how they affected sales in each market. Doing this is expensive and slow. Indeed, test marketing is so expensive and time-consuming that it is mostly used to test new products, not to test different ad campaigns for the same product.[162]

The most flexible way to test ads before the internet was probably direct mail because an advertiser could create different versions of a mailer and see which ones got better results. This led David Ogilvy, maybe the most accomplished advertiser of all time, to call direct mail his "first love and secret weapon."[163] With most forms of advertising, it's hard to tell if a specific ad actually leads

161. *See supra* notes 53–60 and accompanying text. Indeed, the two are so often connected that they can sometimes be interchangeable. For instance, a few years after Facebook acquired the Atlas ad-serving technology and business from Microsoft, the company gave up on it as a major ad-serving platform and repurposed it for measurement and analytics instead. *See* Allison Schiff, *Facebook Shutters Atlas Ad Server, Ending Its Assault on DoubleClick; Atlas to Live On as Measurement Pixel*, ADEXCHANGER (Nov. 18, 2016, 11:00 AM), https://adexchanger.com/platforms/facebook-shutters-atlas-ad-server-ending-assault-doubleclick-atlas-live-measurement-pixel/ [https://perma.cc/Z5KB-826T].

162. *See, e.g.*, N. D. Cadbury, *When, Where, and How to Test Market*, HARV. BUS. REV. (May 1975), https://hbr.org/1975/05/when-where-and-how-to-test-market [https://perma.cc/U7DE-DW3R].

163. OGILVY, *supra* note 48, at 143.

to any incremental sales, which is why the nineteenth-century department-store magnate John Wanamaker (allegedly) said that "I know half my advertising is wasted, I just don't know which half."[164] Direct mail makes it possible to see these effects directly through A/B testing—trying multiple options on random groups of recipients to see which works better. Is it better, for instance, to offer 56 issues of a magazine for $65 or 29 issues for $29.95? As Ogilvy reported, though the latter brought in less revenue per subscriber, it brought in far more new subscribers, and so 35% more revenue.[165] Though there are inherent limits even to this form of testing because it can be impractical and expensive to send more than a few versions of a mailing while tracking the responses in enough detail to draw meaningful conclusions.

The internet makes it much easier and quicker to do A/B testing,[166] so much so that today it's a standard part of many online companies' playbooks.[167] Google famously tests individual aspects of its web design to see, for instance, which of forty-one shades of blue got users to click more often—a level of micromanagement that eventually drove away the company's first visual designer.[168] That example happened a decade ago, though, and things have advanced quickly since then. In the political realm, for instance,

---

164. *E.g.*, Catherine Tucker, *The Implications of Improved Attribution and Measurability for Antitrust and Privacy in Online Advertising Markets*, 20 GEO. MASON L. REV. 1025, 1026 (2013). Versions of the quotation have also been attributed to others, including Henry Ford and Lord Leverhulme. *See id.* at 1026 n.6 (citing Torin Douglas, *Tough Sell for Britain's Mad Men?*, BBC NEWS (Nov. 2, 2010), https://www.bbc.co.uk/news/uk-11674865 [https://perma.cc/PL3Q-HAN6]).

165. OGILVY, *supra* note 48, at 144.

166. I use the term A/B testing because it is the most commonly used term in industry, even though modern implementations routinely compare more than two options. There are plenty of other names for the same thing. *See, e.g.*, RON KOHAVI ET AL., PRACTICAL GUIDE TO CONTROLLED EXPERIMENTS ON THE WEB: LISTEN TO YOUR CUSTOMERS NOT TO THE HIPPO 959, 961 (2007), https://ai.stanford.edu/~ronnyk/2007GuideControlledExperiments.pdf [https://perma.cc/Q2EQ-YASL] ("The web provides an unprecedented opportunity to evaluate ideas quickly using controlled experiments, also called randomized experiments (single-factor or factorial designs), A/B tests (and their generalizations), split tests, Control/Treatment tests, and parallel flights."). If you're curious, HiPPO stands for "Highest Paid Person's Opinion." *Id.* at 959.

167. *E.g.*, Brian Christian, *The A/B Test: Inside the Technology That's Changing the Rules of Business*, WIRED (Apr. 25, 2012, 8:47 PM), https://www.wired.com/2012/04/ff-abtesting/ [https://perma.cc/5FJL-EHTM].

168. *See* Douglas Bowman, *Goodbye, Google*, STOPDESIGN (Mar. 20, 2009), https://stopdesign.com/archive/2009/03/20/goodbye-google.html [https://perma.cc/J9B5-7TH8]; Laura M. Holson, *Putting a Bolder Face on Google*, N.Y. TIMES, Mar. 1, 2009, SundayBusiness, at 1. Google does thousands of tests a year. *See* Jenna Hanington, *The ABCs of A/B Testing*, SALESFORCE PARDOT (July 12, 2012), https://www.pardot.com/blog/abcs-ab-testing/ [https://perma.cc/76FD-U26M] (reporting that Google did more than 7,000 A/B tests in 2011).

Barack Obama's presidential campaigns made extensive use of A/B testing, comparing everything from different website splash pages to different language asking contributors to save their payment information for next time. "Now save your payment information" worked 20–30% better than "Save your payment details now to make the process quicker next time," and these differences, in the aggregate, raised tens of millions of dollars.[169] The Trump campaign took this even further, testing as many as 175,000 different Facebook ads *per day* to see which ones worked best.[170] That speed and scale would be simply impossible with mailers, let alone tv or print advertising.

It's not a coincidence that all the examples in the last paragraph are from large, well-funded companies and organizations, but as with many products and services, the technology underlying A/B testing is evolving from expensive custom services to cheap commodity products. When Amazon did A/B testing for every tweak of its homepage in the early 2000s or when the Obama campaign did its testing in 2008, they basically had to roll their own—creating both the content to test and the infrastructure to test it.[171] Since then, new tools have made it easier to do both. The e-mail-marketing firm MailChimp, for instance, now offers a tool to do A/B testing of e-mail subject lines, "from" names, delivery dates and times, and content;[172] likewise, after the Obama campaign ended in 2008, its head of analytics cofounded Optimizely, a company that makes tools to test website

169. David Moth, *Seven Lessons Obama's Digital Team Learned from A/B Testing Emails*, ECONSULTANCY (Oct. 28, 2013), https://econsultancy.com/blog/63672-seven-lessons-obama-s-digital-team-learned-from-a-b-testing-emails [https://perma.cc/F6PT-7H69]; *see also* Christian, *supra* note 167 (describing how Dan Siroker, previously a product manager at Google, introduced A/B testing to Obama's 2008 campaign).

170. *See, e.g.*, Sarah Frier, *Trump's Campaign Said It Was Better at Facebook. Facebook Agrees*, BLOOMBERG (Apr. 3, 2018, 6:32 PM), https://www.bloomberg.com/news/articles/2018-04-03/trump-s-campaign-said-it-was-better-at-facebook-facebook-agrees [https://perma.cc/QQ4W-K3VS] (reporting that, according to an internal Facebook white paper, the Trump campaign ran 5.9 million different Facebook ads during the 2016 presidential campaign, compared to the Clinton campaign's 66,000); Lapowsky, *supra* note 62 (reporting that tests peaked at 175,000 ads on the day of the third presidential debate); Lesley Stahl, *Facebook "Embeds," Russia and the Trump Campaign's Secret Weapon*, CBS NEWS (Oct. 8, 2017), https://www.cbsnews.com/news/facebook-embeds-russia-and-the-trump-campaigns-secret-weapon/ [https://perma.cc/YR9S-LC8G] (reporting that the campaign tested an average of 50,000 to 60,000 ads per day).

171. *See, e.g.*, KOHAVI ET AL., *supra* note 166, at 959; Dan Siroker, *How Obama Raised $60 Million by Running a Simple Experiment*, OPTIMIZELY BLOG (Nov. 29, 2010), https://blog.optimizely.com/2010/11/29/how-obama-raised-60-million-by-running-a-simple-experiment/ [https://perma.cc/UKL7-APS8].

172. *A/B Testing: See What Works Best*, MAILCHIMP, https://mailchimp.com/features/ab-testing/ [https://perma.cc/V9CX-W5EP] (last visited Sept. 12, 2019).

and mobile-app content.[173] When the Trump campaign did their testing in 2016, they used Facebook's advertising API,[174] which gave them the infrastructure to run and evaluate thousands of different ads, but they still had to build a system to generate thousands of ad contenders and evaluate their results.[175] Since the election, though, Google, YouTube, and Facebook have launched tools that let advertisers automatically generate and test different versions of an ad.[176] Facebook's version, for instance, lets an advertiser provide different ad assets—say, five banner images, three titles, three sets of ad copy, and two links—and automatically generate dozens of versions.[177] A technique, then, that just a few years ago was limited to large, tech-savvy organizations is now available to any online advertiser—including scammers.

This discussion has focused on advertising used to promote scams, but the same story can be told about the rest of the scam as well. Just like tools allowing advertisers to compare different

---

173. *See* Laurie Segall, *Optimizely Aims to Give Obama 2012 a Data Edge*, CNN MONEY (May 2, 2012, 5:24 PM), https://money.cnn.com/2012/04/23/technology/startups/optimizely-election/ [https://perma.cc/6HQ9-A8EH]; Siroker, *supra* note 171. There are plenty more where those came from. *See, e.g.*, Jacob McMillen, *The 20 Most Recommended AB Testing Tools by Leading CRO Experts*, CONVERSION SCI. (Sept. 16, 2016), https://conversionsciences.com/blog/ab-testing-tools/ [https://perma.cc/Q6DV-ESCT].

174. API stands for application programming interface. An API is essentially a tool that allows third parties to write software to interact with a system. Facebook's advertising API, for instance, lets advertisers write their own code to generate, test, and run ads, without any Facebook employees having to be involved directly. *Dynamic Creative*, FACEBOOK FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/dynamic-creative/overview [https://perma.cc/94ER-59WQ] (last visited Sept. 12, 2019).

175. *See, e.g.*, Sue Halpern, *How He Used Facebook to Win*, N.Y. REV. BOOKS, 59–60 (2017) (book review). Facebook has an A/B testing tool, but it's pretty primitive. *See About Split Testing*, FACEBOOK BUS., https://www.facebook.com/business/help/1738164643098669 [https://perma.cc/35YF-93G7] (last updated Apr. 19, 2019). Facebook's only tool for dynamically generated ad content is designed for showing different products to different users from a catalog provided by the advertiser—not really the goal when a campaign is trying to figure out which ads drive donations or votes.

176. *See, e.g.*, Lauren Johnson, *YouTube's Technology Can Now Spit out Thousands of Different Video Ads at Once*, ADWEEK (Sept. 25, 2017), https://www.adweek.com/digital/youtubes-technology-can-now-spit-out-thousands-of-different-video-ads-at-once/ [https://perma.cc/T2YE-R9L5]; Ginny Marvin, *Google AdWords' Automated Ad Suggestions Test Is Getting a Reboot*, SEARCH ENGINE LAND (Sept. 5, 2017, 11:05 AM), https://searchengineland.com/google-adwords-automated-ad-suggestions-beta-281924 [https://perma.cc/KP52-VTEH]; Ginny Marvin, *Google's New Responsive Search Ads Can Show 3 Headlines, Longer Descriptions*, SEARCH ENGINE LAND (May 4, 2018, 11:40 AM), https://searchengineland.com/google-adwords-new-responsive-search-ads-can-show-3-headlines-297428 [https://perma.cc/7BWG-HW3G]; Tim Peterson, *Facebook's Dynamic Creative Can Generate up to 6,250 Versions of an Ad*, MARKETING LAND (Oct. 30, 2017, 8:30 AM), https://marketingland.com/facebooks-dynamic-creative-option-can-automatically-produce-6250-versions-ad-227250 [https://perma.cc/5GEY-HF5R].

177. *See Dynamic Creative*, *supra* note 174; Peterson, *supra* note 176.

ads, tools to compare website and mobile-app content have become cheap and easy to use. A motivated scammer, then, could test different versions of a scam's landing page to see which one snags the most victims—something that took the Obama campaign a lot of effort in 2007 and 2008, but is now easy to do with off-the-shelf components. Indeed, we may be approaching the point where the comparison isn't even necessary, if an AI can just tell you the best ad to begin with.[178]

Individualized Scams. The final way that targeting platforms make it easier to scam people is by making it possible to tailor scams to individual victims. This is a culmination of the tracking and testing techniques discussed in the rest of this Part: instead of just using tracking tools to show ads to the most interested audiences,[179] or just using A/B testing to figure out which ads are most effective,[180] why not combine them to show each interested individual the version of the scam that would be most persuasive to that individual victim? Classic A/B testing tells you which option works best in the aggregate, but if you can figure out that option A works better on some people while option B works better on others, there's no reason not to make use of that information.

Just as large-scale tracking and testing are difficult or impossible without the internet, large-scale individualized scams are impossible to pull off without the sorts of tools provided by tracking platforms. Indeed, they're far harder to pull off together than tracking and testing are individually because the number of variables in play is far higher. Instead of just analyzing, say, 200 user-specific variables to determine which users should see an ad, or 200 ad-specific variables to determine which version of an ad works best, a system would need to analyze how each of the 200 user-specific variables interacts with each of the 200 ad-specific variables—40,000 combinations. The math is far more complicated, and because search space grows exponentially with the number of dimensions, ungodly amounts of data can be needed to make reliable predictions.[181]

178. *See, e.g.*, Emily Alford, *How AI Could Make A/B Testing a Thing of the Past*, CLICKZ (Aug. 10, 2018), https://www.clickz.com/how-ai-could-make-a-b-testing-a-thing-of-the-past/216302/ [https://perma.cc/77BV-4XRW].

179. *See supra* Section III.B.1.

180. *See supra* Section III.B.3.

181. This is all highly simplified. For more, see, for example, KEVIN P. MURPHY, MACHINE LEARNING: A PROBABILISTIC PERSPECTIVE 1–25 (2012) (describing the scope and basic requirements of machine learning, including the need for sufficient training data across the search space of inputs and the curse of dimensionality, wherein that search space increases exponentially with the number of dimensions).

Even modern targeting systems, then, don't often target individual users with individual versions of an ad. Advertisers instead have had to do it manually, using the results of testing to set up different campaigns when results indicate different ads might be effective for different groups of users. In the last year or two, though, tools like machine learning and especially deep learning are starting to make it possible. Machine learning is a broad term that encompasses many different techniques,[182] but several of those approaches are well suited for the challenge because they can deal with very-high-dimensional data.[183] A deep neural network, for instance, can take data with hundreds or thousands of dimensions, like the browsing behavior and personal information about users and whether or not those users responded to different ads, and boil it down to a small number of variables that predict nearly all the variance.[184] Using this technology to predict which users are most likely to click on an ad is becoming old hat.[185] Combining it with individualized ads is in its infancy,

182. *See, e.g.*, Brandon Wirtz, *8 AI Technologies That Ain't Neural Networks*, LINKEDIN (Jan. 28, 2018), https://www.linkedin.com/pulse/8-ai-technologies-aint-neural-networks-brandon-wirtz/ [https://perma.cc/M4WL-MQZF].

183. *See, e.g.*, JOHN D. KELLEHER ET AL., FUNDAMENTALS OF MACHINE LEARNING FOR PREDICTIVE DATA ANALYTICS: ALGORITHMS, WORKED EXAMPLES, AND CASE STUDIES 226–37, 249–69 (2015) (describing how approaches like feature selection and Bayesian modeling can get around the curse of dimensionality). This is a small sampling of approaches; for a review of many more, see, for example, C.O.S. Sorzano et al., *A Survey of Dimensionality Reduction Techniques* (arXiv, Working Paper No. 1403.2877v1, 2014), https://arxiv.org/pdf/1403.2877 [https://perma.cc/L22P-K7VF]. For a nicely accessible lay explanation of the problem, see Nikhil Buduma, *The Curse of Dimensionality and the Autoencoder*, MUSINGS MIT STUDENT (Mar. 10, 2015), http://nikhilbuduma.com/2015/03/10/the-curse-of-dimensionality/ [https://perma.cc/492T-ZLSE].

184. *See, e.g.*, Jürgen Schmidhuber, *Deep Learning in Neural Networks: An Overview*, 61 NEURAL NETWORKS 85, 94 (2015). For accessible lay explanations, see Nikhil Buduma, *A Deep Dive into Recurrent Neural Nets*, MUSINGS MIT STUDENT (Jan. 11, 2015), http://nikhilbuduma.com/2015/01/11/a-deep-dive-into-recurrent-neural-networks/ [https://perma.cc/UFW4-75H6]; Nikhil Buduma, *Deep Learning in a Nutshell*, MUSINGS MIT STUDENT (Dec. 29, 2014), http://nikhilbuduma.com/2014/12/29/deep-learning-in-a-nutshell/ [https://perma.cc/FHC3-TCNK].

185. *See, e.g.*, Tom Simonite, *Google and Microsoft Can Use AI to Extract Many More Ad Dollars from Our Clicks*, WIRED (Aug. 31, 2017, 7:00 AM), https://www.wired.com/story/big-tech-can-use-ai-to-extract-many-more-ad-dollars-from-our-clicks/ (discussing Google and Microsoft's use of deep learning to generate ad clicks) [https://perma.cc/7RZE-QBZJ]; Marty Swant, *Snapchat Is Beginning to Use Machine Learning to Improve Ad Targeting*, ADWEEK (Dec. 30, 2016), https://www.adweek.com/digital/snapchat-beginning-use-machine-learning-improve-ad-targeting-175330/ [https://perma.cc/ST77-RGMT] (explaining how Snapchat uses machine learning for its API); Sridhar Ramaswamy, *Powering Ads and Analytics Innovations with Machine Learning*, INSIDE ADWORDS (May 23, 2017), https://adwords.googleblog.com/2017/05/powering-ads-and-analytics-innovations.html (describing machine-learning-based tools to target customers who are actively in the market for a major purchase and identify those who are closest to purchasing); Guorui Zhou et al., *Deep Interest Network for Click-Through Rate Prediction* 2–5 (arXiv, Working Paper No. 1706.06978v4,

but almost certain to grow quickly.[186] Soon, then, it will be trivial for a scammer to show different ads to different potential victims, each automatically optimized to ensnare that particular victim.

IV. INTERVENTIONS

If targeting platforms make it easier to commit scams and harder to detect them, then counteracting these effects could pay significant dividends for consumers. One naïve approach would be to ban targeting for these purposes, or even for all purposes.[187] But because targeting is so entrenched and, arguably, has so many other legitimate uses, banning it is likely to be politically unviable and enforcement would be difficult.[188] Another naïve approach would be to invest more resources into investigation and detection. This would quickly turn, though, into an expensive cat-and-mouse game between scammers and investigators.[189] Moreover, even if these approaches could work, neither is well tailored to the unique features of online targeting platforms.

A promising approach could instead be to use targeting to fight the downsides of targeting: using the same tools that enable targeted scams to detect and prevent them. The same targeting technologies that make it possible to identify the most promising potential victims, for instance, could provide new ways to detect and block scams by revealing their own characteristic patterns.

2018), https://arxiv.org/abs/1706.06978 [https://perma.cc/ZM8V-N8NP] (reporting a deep neural network used by the Chinese retailer Alibaba to predict click-through rates); Ruoxi Wang et al., *Deep & Cross Network for Ad Click Predictions* 4, 6 (arXiv, Working Paper No. 1708.05123v1, 2017), https://arxiv.org/abs/1708.05123 [https://perma.cc/D6BE-QBAW] (similar use, but for Google).

186. In July 2018, for instance, Google announced "responsive search ads," a new ad format in which an advertiser provides different options for the ad's headline and description and Google uses machine learning to predict which combination works best for a given user making a given search query. *See* Jerry Dischler, *Putting Machine Learning into the Hands of Every Advertiser*, GOOGLE (July 10, 2018), https://blog.google/technology/ads/machine-learning-hands-advertisers/ [https://perma.cc/GQ8Q-JVQ9].

187. *See, e.g.*, David Dayen, *Ban Targeted Advertising*, NEW REPUBLIC (Apr. 10, 2018) https://newrepublic.com/article/147887/ban-targeted-advertising-facebook-google [https://perma.cc/AU4L-3S7C]; Harper Neidig, *Lawmakers Roll out Bill to Protect Children from Online Data Collection*, HILL (May 23, 2018, 4:46 PM), http://thehill.com/policy/technology/389077-lawmakers-push-bill-to-protect-children-from-online-data-collection [https://perma.cc/FMC6-EL6F].

188. *See, e.g.*, Neidig, *supra* note 187 (noting that a bipartisan bill to ban targeted advertising to children has been introduced "several times over the past decade, with little success").

189. *See, e.g.*, Dan Turkel, *Hackers Are Playing a 'Cat-and-Mouse Game' with the IRS—and Doing an 'Amazingly' Good Job at Stealing Your Tax Returns*, BUS. INSIDER (Feb. 24, 2016, 6:49 PM), https://www.businessinsider.com/the-irs-is-warning-of-increased-fraud-phishing-attempts-this-tax-season-2016-2 [https://perma.cc/2BRY-GXNJ].

This would, effectively, provide a new means of investigation and detection specific to data scams. There are two basic ways these tools could come about: platforms could make it possible for law-enforcement authorities to deploy and use these tools to stop scams, or the platforms could do it themselves. Both approaches, though, face substantial—maybe even disqualifying—obstacles.

A. Using Technology to Detect and Prevent Scams

Because the problem of data scams is, at its root, technological, one obvious approach is to look to technology for solutions to that problem. There are reasons to think that the data and targeting technologies that make targeting platforms possible could help detect and prevent scams.

There are many ways technology might be used to detect and prevent scams. Someone developing a scam-detection tool might compare known scams to innocent behavior, for instance, and look for patterns that might indicate scams.[190] Or they might look for ways to identify especially gullible or vulnerable users and see who is targeting those users.[191] Or they might look for short-term advertisers that switch from account to account, or just subject new advertisers to extra scrutiny.[192] Or they might examine those ads that gain popularity quickly.[193] The right tools and techniques

190. For example, Apple detected a violation of the iOS App Store's terms by the Uber app because the app was set up to behave differently when it was physically located at Apple's headquarters. Mike Isaac, *Uber's C.E.O. Plays with Fire*, N.Y. TIMES (Apr. 23, 2017), https://www.nytimes.com/2017/04/23/technology/travis-kalanick-pushes-uber-and-himself-to-the-precipice.html [https://perma.cc/6C7Q-GK5E]. This is behavior indicative of a scam, because there's no good reason to behave differently at precisely the one location where software is reviewed for approval to appear on Apple's App Store platform. It's also the sort of thing that a platform could—and did—detect using its own analytics tools.

191. For example, some companies are now sending their employees fake phishing e-mails to see which employees click on them. When a user clicks on such an e-mail, they get a page explaining the threat of phishing. *See, e.g.*, Barbara Ortutay, *Companies Send Fake Phishing Emails to Test Security*, PRESS HERALD (Feb. 12, 2015), https://www.pressherald.com/2015/02/12/companies-send-fake-phishing-emails-to-test-security/ [https://perma.cc/VWC2-Y8MW]. Likewise, an advertising platform like Google or Facebook could, if it wanted, post implausible fake ads and see who clicks on them; or they could look for other indicators of gullibility, like buying nose-hair trimmers. *See supra* note 52 and accompanying text.

192. For example, Facebook recently announced added scrutiny for political advertisers and users who run popular groups, requiring that their identities be verified before they can advertise or post. Rob Goldman & Alex Himel, *Making Ads and Pages More Transparent*, FACEBOOK NEWSROOM (Apr. 6, 2018), https://newsroom.fb.com/news/2018/04/transparent-ads-and-pages/ [https://perma.cc/4646-ZR5C]. This makes it harder for a scammer to account-hop—at least for a scam with a political element, like the American Horizons scam—or to set up a scam group while hiding behind a fake identity.

193. Such a burst of popularity can be a sign that someone is paying a click farm to increase traffic artificially, for instance by reviewing a product or following a social-media

will change quickly as scammers adapt and technology develops—but the same is true of the underlying targeting tools and techniques.

Indeed, companies have demonstrated a remarkable ability to detect scams using data and, especially, machine learning. Banks, insurance companies, and other businesses have worked for decades to identify fraudulent transactions.[194] More recently, online stores and platforms have tried to do the same thing. Fraud is especially problematic for online stores because thieves can use orders to monetize stolen credit or debit cards, shipping goods to mail drops or vacant addresses, and then collecting them for use or resale. Once an item is shipped, there's no getting it back from a thief, even though the store typically gives up the revenue on fraudulent transactions due to credit-card chargebacks. Online stores have strong reason, then, to predict fraudulent transactions before they happen, and a vibrant industry has emerged of companies with names like Riskified, Signifyd, and Accertify that promise to make such predictions.[195]

Some of the most interesting fraud-detection cases arise in two-sided platform markets—platforms that act as intermediaries bringing together both sides of a transaction, like eBay (buyers and sellers) or Uber (drivers and passengers) or even dating sites.[196] These platforms have to deal with customers on either side trying to defraud the platform as well as customers trying to defraud their counterparties. Uber estimates, for example, that fraudulent trips make up as much as 10% of bookings when it enters a market; with time, the company can bring that down to "sustainable" levels of around 0.5%.[197] (These frauds work in

account or clicking on an ad. *See, e.g.*, Laura Stevens & Jon Emont, *To Game Amazon, Sellers Use Scams, Clicks & Dirty Tricks*, WALL ST. J., July 28, 2018, at B1–B2; Vijaya Gadde, *Confidence in Follower Counts*, TWITTER BLOG (July 11, 2018), https://blog.twitter.com/official/en_us/topics/company/2018/Confidence-in-Follower-Counts.html [https://perma.cc/W5PW-AK6Y]; Charles C. Mann, *How Click Fraud Could Swallow the Internet*, WIRED (Jan. 1, 2006, 12:00 PM), https://www.wired.com/2006/01/fraud/ [https://perma.cc/44QA-JLEY].

194. *See, e.g.*, Aisha Abdallah et al., *Fraud Detection System: A Survey*, 68 J. NETWORK & COMPUTER APPLICATIONS 90, 92–94 (2016); Richard J. Bolton & David J. Hand, *Statistical Fraud Detection: A Review*, 17 STAT. SCI. 235, 237–45 (2002); E.W.T. Ngai et al., *The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework and an Academic Review of Literature*, 50 DECISION SUPPORT SYS. 559, 562–64 (2011); Jarrod West & Maumita Bhattacharya, *Intelligent Financial Fraud Detection: A Comprehensive Review*, 57 COMPUTERS & SECURITY 47, 50–56 (2016).

195. *See* Safdar, *supra* note 154.

196. *See, e.g.*, Jennifer Levitz, *Online Daters Are Falling Prey to Scams*, WALL ST. J., Sept. 1, 2016, at A3.

197. *One Driver Explains How He Is Helping to Rip off Uber in China,* BLOOMBERG, (June 28, 2015, 6:40 PM), https://www.bloomberg.com/news/articles/2015-06-28/one-driver-

various ways. Some drivers buy modified phones that can use multiple SIM cards and phone numbers, so they can both request a ride as a passenger and accept the ride as a driver from the same phone.[198] Sometimes these rides are billed to a stolen credit card, but sometimes they're legitimately paid for, taking advantage of new-customer bonuses that mean that Uber sometimes pays a driver more than it charges a rider.[199] Some drivers add in GPS-spoofing tools to go on "rides" that were never actually taken.[200] Uber has devoted substantial resources to detecting new forms of fraud, looking for patterns like trips where the driver's phone indicated a GPS altitude that would mean that the car was flying, or trips where the car went substantially faster than other nearby cars through crowded city streets, or users who spent more time adding and deleting payment methods than comparing prices for different levels of service.[201] This isn't foolproof because the line between fraud and reasonable customer service can be fuzzy,[202] but instances like the flying cars are unambiguous. Once certain trips have been classified as fraudulent, the company can use that fact to learn more: instead of terminating a user committing fraud, it has sometimes allowed it to continue for a time, building a dataset of known-fraudulent trips that can be used to find new patterns using machine learning.[203]

The successes that companies have had in detecting fraud suggests that using similar technologies might be able to use data to detect scams. This would allow someone—maybe law-enforcement authorities, or maybe the platforms themselves—to shut them down or even block them before they victimize anyone.

---

explains-how-he-is-helping-to-rip-off-uber-in-china [https://perma.cc/4TSD-CDF4].

198. *Id.*

199. Alistair Charlton, *Uber Taken for a Ride by Scammer Drivers Earning Profit from Bogus Fares*, INT'L BUS. TIMES (June 30, 2015, 12:36 PM), https://www.ibtimes.co.uk/uber-taken-ride-by-scammer-drivers-earning-profit-bogus-fares-1508601 [https://perma.cc/6BTY-ZV4K]; Alfred Ng, *Uber Fights Off Scammers Every Day. Here's How It Learned the Tricks*, CNET (June 14, 2018, 5:00 AM), https://www.cnet.com/news/uber-fights-off-scammers-every-day-heres-how-it-learned-the-tricks/.

200. Ng, *supra* note 199.

201. *See, e.g.*, *id.*; Ting Chen, *Advanced Technologies for Detecting and Preventing Fraud at Uber*, UBER ENGINEERING BLOG (Jan. 14, 2018), https://eng.uber.com/advanced-technologies-detecting-preventing-fraud-uber/ [https://perma.cc/P3UB-ZU6D].

202. *See, e.g.*, Greg Bensinger, *Uber Drivers Take Riders the Long Way—at Uber's Expense*, WALL ST. J., (Aug. 13, 2018, 6:44 PM), https://www.wsj.com/articles/uber-drivers-take-riders-the-long-wayat-ubers-expense-1534152602 [https://perma.cc/R5XC-R4EN] (reporting a common scam in which Uber drivers take passengers on slightly-longer-than-optimal routes—sometimes citing traffic or construction as an excuse—to take advantage of Uber's pricing structure, under which passengers pay fixed prices but drivers are paid according to a ride's distance and duration).

203. Ng, *supra* note 199.

The hard question, though, is who can and should develop and deploy such tools.

B. Giving Law-Enforcement Agencies Tools to Stop Scams

One obvious candidate to develop and deploy these scam-detection tools is the same group of law-enforcement authorities that go after scams in the first place. There are reasons to think these agencies would be well-suited to the task, but there are also reasons to be skeptical of this approach. Law-enforcement agencies might have strong incentives to detect and prevent scams, both because that's part of their mission and because they can obtain bureaucratic benefits from successes. They also have domain expertise in frauds and scams, which might help develop better scam-detection tools, and in investigations and the criminal-justice system, which might help them know which scams to prioritize and what to do once one has been detected. At the same time, they may lack the expertise in platform technologies, data analytics, machine learning, and other technologies that might be critical to developing scam-detection tools. There are occasional exceptions like the FBI's Operational Technology Division, which develops and deploys precisely this sort of investigative technology, but those exceptions are unlikely to match the sheer volume of online communications and potential scams.[204] Even when an agency does have skilled technical staff, using a platform's tools can mean two layers of technical staff and infrastructure, and so double the opportunities for something to go wrong. A key challenge in implementing law-enforcement tools, then, will be overcoming that lack of technical expertise.

There are many ways that agencies could structure scam-detection tools to look for targeted scams, requiring different degrees of technical sophistication and cooperation from platforms. At one end of the spectrum, an agency could just flag known scams for platforms, providing hashes or search terms or other indicators of suspicious behavior and asking platform operators to block scams or refer them to the agency. Similar techniques are already used to search for copyright infringement

204. *See Operational Technology*, FBI, https://www.fbi.gov/services/operational-technology [https://perma.cc/MD47-NBQK] (last visited Sept. 12, 2019) ("The Operational Technology Division (OTD) . . . develops and deploys technology-based solutions to enable and enhance the FBI's intelligence, national security, and law enforcement operations. . . . While OTD's work doesn't typically make the news, the fruits of its labor are evident in the busted child pornography ring, the exposed computer hacker, the prevented bombing, the averted terrorist plot, and the prosecuted corrupt official.").

and child pornography,[205] and these techniques could be expanded to scams that agencies could readily identify and characterize in unambiguous terms.

An intermediate method might be for a platform operator to set up a portal through which agencies could see relevant platform data in real time. Such a portal could provide, for instance, running lists of the most commonly targeted demographics or the most frequently clicked ads.[206] This would give agencies a high-level overview of activity on a platform without handing over access to the underlying data; agencies could use this overview to track trends and look for targeting that might indicate a scam.

The most aggressive approach might involve a platform creating an API through which agencies could perform their own analysis of targeting data.[207] This would let agencies develop their own tools and do their own data analysis to find scams, leveraging their expertise in frauds and scams. It might also allow agencies to combine information they obtain using a platform's API with information they have from other sources, which could help them track down scammers who might otherwise escape attention.

---

205. On copyright, YouTube runs Content ID, a private system for tagging copyrighted works. *See, e.g.*, *How Content ID Works*, YOUTUBE HELP, https://support.google.com/youtube/answer/2797370 [https://perma.cc/K43F-T5Q7] (last visited Sept. 12, 2019). On child pornography, the National Center for Missing & Exploited Children (NCMEC) runs a database of hashes of known images of child pornography, which online service providers can use to scan for child pornography uploaded or transmitted by users. *See, e.g.*, Sean Gallagher, *How Verizon Found Child Pornography in Its Cloud*, ARS TECHNICA (Mar. 5, 2013, 10:51 AM), https://arstechnica.com/information-technology/2013/03/how-verizon-found-a-child-pornographer-in-its-cloud/ [https://perma.cc/CMH2-44JT]. Under federal law, service providers are obligated to report known instances of child pornography to NCMEC, and both they and the NCMEC are immune from liability for doing so. *See* 18 U.S.C. §§ 2258A–2258E (2012).

206. There are many such law-enforcement portals for many different purposes. Google, for instance, runs a portal called LERS, the Law Enforcement Request System, through which agencies can request user information. *Law Enforcement Request System*, GOOGLE, https://lers.google.com/ [https://perma.cc/BJN5-9867] (last visited Sept. 12, 2019). Other platforms have similar tools. There are also portals and databases used to track stolen goods, like LeadsOnline, which lets agencies search eBay listings and sales, transactions reported by pawn shops, and transactions involving ingredients and tools needed to run a meth lab. *See LeadsOnline: Services*, LEADSONLINE, https://www.leadsonline.com/main/services.php [https://perma.cc/8WGN-5DS4] (last visited Sept. 12, 2019). There are also tools for agencies to get information needed to track down a suspect or serve a subpoena, for instance based on a phone number. *E.g.*, *Numbering Data at Your Fingertips*, NPAC, https://lawenforcement.numberportability.com/ [https://perma.cc/3FW6-WDCV] (last visited Sept. 12, 2019).

207. There is some overlap with the previous category. The Enhanced Law Enforcement Platform from the U.S. Number Portability Administration Center, for instance, provides web and API access to information about a phone number. *ELEP Service*, NPAC, https://lawenforcement.numberportability.com/services/elep/ [https://perma.cc/Z5ST-FBUJ] (last visited Sept. 12, 2019).

These are just some examples; plenty of other options are possible, like query-based visualization or modeling software that could let agencies investigate targeting without access to the underlying data.

The most aggressive approaches provide the most power, but they also would require giving agencies access to a tremendous amount of information. The specifics of the toolset matter greatly because different tools might give agencies wildly different views of a platform's activity. Whatever the details, though, most of these options would require some amount of cooperation from platform operators. And it's far from clear that they would be willing to cooperate: while platforms might be happy to let agencies do the heavy lifting of detecting and preventing scams, they also have reasons they might resist. For example, when information leaked about PRISM, an NSA program to collect information from platform companies, those companies disclaimed knowledge of the collections and likely became less willing to cooperate with government agencies in the future.[208] Likewise, when the FBI demanded that Apple create a back door to unlock a suspect's iPhone, it caused the company to dig in publicly and explain why it fought a court order to do so.[209] When the Department of Housing and Urban Development went after Facebook for alleged housing discrimination, settlement negotiations broke down, Facebook claimed, over HUD's demand for access to Facebook user information.[210] Public criticism in 2016 led Twitter to ban law-enforcement use of the platform's API for surveillance—of suspects or (per press reports) political protesters—and to cut off third parties that helped agencies use it for this purpose.[211] Platforms have not been reluctant to withhold access

208. *See* Frederic Lardinois, *Google, Facebook, Dropbox, Yahoo, Microsoft, Paltalk, AOL and Apple Deny Participation in NSA PRISM Surveillance Program*, TECH CRUNCH (June 6, 2013), https://techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/ [https://perma.cc/45F2-XZ6L].

209. Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), https://www.apple.com/customer-letter/ [https://perma.cc/CFK2-GNFE].

210. Russell Brandom, *Facebook Has Been Charged with Housing Discrimination by the US Government*, VERGE (Mar. 28, 2019, 7:51 AM), https://www.theverge.com/2019/3/28/18285178/facebook-hud-lawsuit-fair-housing-discrimination [https://perma.cc/34AA-KCB8].

211. *See, e.g.*, Kate Conger, *Twitter Cuts Dataminr Access for Law Enforcement Fusion Centers*, TECH CRUNCH (Dec. 15, 2016), https://techcrunch.com/2016/12/15/twitter-cuts-dataminr-access-for-law-enforcement-fusion-centers/ [https://perma.cc/7B6N-EP6H]; Chris Moody, *Developer Policies to Protect People's Voices on Twitter*, TWITTER DEVELOPER BLOG (Nov. 22, 2016), https://blog.twitter.com/developer/en_us/topics/community/2016/developer-policies-to-protect-peoples-voices-on-twitter.html [https://perma.cc/QGZ5-SRQU]; Timothy J. Seppala, *Twitter Says No to Law Enforcement Protest Policing Tool*, ENGADGET (Dec. 10, 2016), https://www.engadget.com/2016/12/10/twitter-says-no-to-law-enforcement-protest-policing-tool/ [https://perma.cc/6FVN-NP4V].

to their information and APIs; when weighing the costs and benefits of helping agencies fight scams, they might conclude that the costs outweigh the benefits.

Platforms might be especially hesitant to cooperate with agencies because anything that gives agencies access to user information would create substantial privacy and civil-liberties risks. Different scam-detection tools would have different implications, but the common denominator is that some information about a platform's users will wind up in agencies' hands. If a social network creates an API that lets agencies examine and process raw targeting information, for instance, that might include information about users' photos, friend networks, interests, posts and comments, and private chats—plus anything the platform is able to infer about the user through her browsing behavior, IP address, geolocation information, and so forth. Some of this information will not be especially sensitive, but some of it will be, and even seemingly nonsensitive information can reveal a tremendous amount when considered in the aggregate.

These privacy issues could create legal problems for platforms. Platform companies with competent lawyers will have privacy policies that are broad enough to allow information sharing with law-enforcement agencies, so under the dominant notice-and-consent privacy regime in the United States, this kind of sharing may be fine. A broad privacy policy wouldn't necessarily immunize a company against all legal troubles, though; the FTC, for instance, looks beyond fine-print policies to a company's representations in its marketing and communications with users.[212] Multinational companies would also have to consider how cooperation would be treated by European regulators and courts under the General Data Protection Regulation.[213] And a platform's privacy policy does nothing for government agencies, which are bound by constitutional and statutory privacy protections. The Wiretap Act and Stored Communications Act, for instance, limit the government's power to obtain electronic communications without a court order or consent of the parties to the communication.[214] Though obtaining information held by third

212. *See, e.g.*, Solove & Hartzog, *supra* note 88, at 629–30.

213. In striking down the Safe Harbor agreement between the European Union and the United States, for instance, the European Court of Justice concluded that national-security concerns were insufficient to trump the fundamental right to privacy. *See* Case C-362/14, Schrems v. Data Prot. Comm'r, 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362 [https://perma.cc/C77H-KVH6].

214. Wiretap Act, 18 U.S.C. §§ 2510–2522 (2012); Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012); *see also* Orin Kerr, *The FCC's Broadband Privacy Regulations*

parties usually does not infringe users' Fourth Amendment rights,[215] the Supreme Court recently rejected the broadest applications of this principle,[216] and one justice previously suggested that a broader rethinking might be necessary.[217]

These difficulties need not be fatal for agency efforts to detect and prevent scams, but they limit the government's options. The law could simply demand that platforms cooperate, though defining the scope and capabilities of the required cooperation would be difficult, especially given the speed with which platforms' technical capabilities change. Gentler forms of encouragement are more likely to work, but only when the benefits to a platform—in avoiding controversy and regulatory scrutiny—outweigh the costs. There are, however, many ways to shift these costs and benefits. Agencies could look to build cooperative relationships with platforms, implicitly dangling the carrot of a close relationship with law enforcement or the stick of an antagonistic relationship. Agencies could also offer more explicit benefits, like money or purchases of a platform's products. If agencies have their own technical expertise, they can offer this expertise and whatever benefits come from technical cooperation; this might be especially useful for smaller platforms. Still, platforms' broader business concerns and public-relations concerns are likely to trump all but the most substantial law-enforcement needs, so alternatives to agencies may be needed.

C. Giving Targeting Platforms Incentives to Stop Scams

Instead of relying on law-enforcement agencies, targeting platforms could go after scams directly. Platform operators could be well positioned to do this because they have the technical capabilities that agencies may lack. These efforts could also be on firmer legal ground than law-enforcement efforts would be. They face other difficulties, though: because platform operators make money when their platforms are used to target people, they have little incentive to shut down what could be whole categories of customers.[218] One potential approach to solving the data-scam

---

Are Gone. But Don't Forget About the Wiretap Act, WASH. POST (Apr. 6, 2017), http://wapo.st/2o0XfA0.

215. Smith v. Maryland, 442 U.S. 735, 742–45 (1979); United States v. Miller, 425 U.S. 435, 442–43 (1976).

216. Carpenter v. United States, 138 S. Ct. 2206, 2219–20 (2018).

217. United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring).

218. A similar dynamic has played out with YouTube's recommendation algorithm. The algorithm optimizes for increasing viewer engagement, but this turns out to reward extremist videos and videos touting conspiracy theories and other deleterious content.

problem, then, would be to increase operators' incentives to detect and prevent scams that use their platforms.

If anyone can develop software tools to detect and prevent data scams, it would include the same people that run targeting platforms in the first place. Those developers are necessarily familiar with the capabilities and architectures of their own platforms, which gives them advantages in extending the platforms to build new capabilities. They're also good at figuring out the right variables to use for targeting and at finding patterns in the data by using machine learning, running A/B tests and experiments, and so forth. Moreover, although platforms lack the native expertise in investigating frauds and scams, such capabilities are probably easier to duplicate than technical expertise because they are more widespread—there are many law-enforcement officers investigating many types of crime—and because retired law-enforcement officers frequently join private industry.[219] Extending targeting platforms to detect scams, then, could be a plausible response to data scams.

At the same time, platforms have little incentive to exclude whole categories of customers, for two reasons. The obvious reason is that doing so would eliminate a source of revenue. This, however, likely plays less of a role than it might seem, because the sheer scale of platforms like Google or Facebook means that any one market segment likely provides a negligible fraction of revenue. Though, if the excluded category of customers is large, then it could have an effect. In recent months, for instance, both Twitter and Facebook saw their stock prices fall dramatically after announcing slowdowns in user growth—in Twitter's case, after revealing that it was deleting tens of millions of fake accounts per

---

YouTube has spent years trying to eliminate this problem, with little sign of major success. The obvious easy solution would be to optimize for something different or get rid of the recommendation algorithm, but the business downsides of that are large enough that YouTube is apparently unwilling to do so. *See, e.g.*, *YouTube's Algorithm Keeps Suggesting Extremist Content*, NEW SCIENTIST, July 13–19, 2019, at 14; Craig Timberg et al., *YouTube Excels at Recommending Videos—but Not at Detecting Hoaxes*, WASH. POST (Feb. 22, 2018), http://wapo.st/2CDWYZB; Kelly Weill, *How YouTube Built a Radicalization Machine for the Far-Right*, DAILY BEAST (Dec. 19, 2018, 10:32 AM), https://www.thedailybeast.com/how-youtube-pulled-these-men-down-a-vortex-of-far-right-hate [https://perma.cc/5SC4-S9A6].

219. *E.g.*, *Occupational Separations and Openings*, U.S. BUREAU OF LAB. STAT., https://www.bls.gov/emp/tables/occupational-separations-and-openings.htm [https://perma.cc/8NE8-5DQX] (last modified June 24, 2019) (estimating that 4.1% of law-enforcement workers would transfer occupations annually between 2016 and 2026); Jerri Williams, *Retired FBI Agents Make Great Second Career Hires: Why I Dyed My Hair Blue*, LINKEDIN (Dec. 11, 2015), https://www.linkedin.com/pulse/retired-fbi-agents-make-great-second-career-hires-why-jerri-williams/ [https://perma.cc/P8RZ-CE22].

month.[220] Moreover, blocking a controversial category of customers can help avoid scrutiny from skeptical outsiders; this may be why Google and Facebook have banned ads for controversial subjects like payday lenders, bail bonds, cryptocurrencies, and unapproved medicines.[221]

The subtler reason platforms have little incentive to exclude categories of customers is that blocking a category of ads isn't automatic; it takes effort and engineering resources to enforce the prohibition. Platforms operate on automation and scale, not laborious individual enforcement. In the copyright context, Google developed Content ID specifically to avoid manually processing millions of copyright takedown demands. Likewise, search engines strenuously fought the European "right to be forgotten" by arguing (among other things) that they were not equipped to decide whether pages should be de-indexed in individual cases. The Court of Justice of the European Union rejected the argument, and now search engines operating in Europe are forced to review individual requests to remove search results that are "inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes [for which they were collected or processed] and in the light of the time that has elapsed."[222] A rule that banned scams would likewise require substantial enforcement resources, both because such a rule is unlikely to provide clear boundaries between permissible and impermissible ads and because scammers are by their nature willing to bend or break the rules.[223] Even if a platform tried to avoid these problems by using machine learning or similar tools to automate enforcement, it would need to continually update its

220. *See* Emily Stewart, *The $120-Billion Reason We Can't Expect Facebook to Police Itself*, VOX (July 28, 2018, 2:04 PM), https://www.vox.com/business-and-finance/2018/7/28/17625218/facebook-stock-price-twitter-earnings [https://perma.cc/5KQX-MW7T]; Craig Timberg & Elizabeth Dwoskin, *Twitter Is Sweeping out Fake Accounts Like Never Before, Putting User Growth at Risk*, WASH. POST (July 6, 2018), https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/.

221. *See, e.g.*, David McCabe, *Google, Facebook to Ban Bail Bond Ads*, AXIOS (May 7, 2018), https://www.axios.com/google-bail-bonds-ads-ban-1525720613-6cde91b2-6938-4273-ab86-e0211ee97292.html [https://perma.cc/8XJS-E4DP]; Ian Wren, *Google Follows Facebook in Banning Cryptocurrency Ads*, NPR (Mar. 14, 2018, 3:24 PM), https://www.npr.org/sections/thetwo-way/2018/03/14/593553255/google-follows-facebook-in-banning-cryptocurrency-ads [https://perma.cc/AP5L-YZ3E]; Andrea Peterson & Jonnelle Marte, *Google to Ban Payday Loan Advertisements*, WASH. POST, (May 11, 2016), http://wapo.st/1T3dY0n.

222. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN [https://perma.cc/YU29-E68R].

223. On the many difficulties in private governance of online platforms, see Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1630–62 (2018).

tools and algorithms as scammers found new loopholes and corner cases.

Given these downsides to blocking scams, targeting platforms are likely to take action on their own against scammers only when it is clearly in their self-interest to do so. Just as when it comes to cooperating with law-enforcement agencies, there are different ways to tweak these incentives. The simplest approach, again, would be to pay platforms directly to root out scams, but as always, there are other approaches with different levels of aggressiveness. An unaggressive approach might encourage platforms to educate users about scams, imposing costs that would fall mostly on platforms that fail to root out scams.[224] A slightly more aggressive approach might involve regulators investigating scammers in ways that impose indirect costs on platforms, perhaps by subpoenaing records or calling executives to testify. A yet-more-aggressive approach would try to hurt platforms' other business until they ban certain categories of advertising. Perhaps the most aggressive option would be to hold companies civilly or criminally liable for scams committed through their platforms. Regulators have plenty of experience using all these tools against online platforms in other contexts like sex trafficking, for good or for ill; there is little reason they could not try to turn them to targeted scams.[225]

Efforts to encourage platforms to block scams have their downsides. For one thing, even setting aside the problem of scale, the challenge would be substantial, since blocking scammers isn't trivial. The lines between scammer and legitimate advertiser can be blurry, especially when that decision must be made by an uninterested company with little reason to investigate the facts. Errors will inevitably prevent some legitimate advertisers from using a platform or permit some scammers to sneak through. The biggest obstacles, though, may be legal, since provisions like the

224. Craigslist, for instance, posts warning messages at the top of its classified ads warning about common scams. It's possible, for what it's worth, that a warning message wouldn't cost a platform operator money in the long run if it increases the platform's trustworthiness and led users to rely more heavily on it. *See, e.g.*, *Avoiding Scams*, CRAIGSLIST, https://www.craigslist.org/about/scams [https://perma.cc/7NM9-AL4P] (last visited Sept. 12, 2019).

225. *See, e.g.*, Backpage.com, LLC v. Dart, 807 F.3d 229, 230–33 (7th Cir. 2015) (detailing Cook County Sheriff Tom Dart's extended efforts to kill Backpage.com's classified ads for adult services). In 2018, Congress enacted new limits on § 230—discussed shortly below—designed to make it easier to shut down websites that enable sex crimes. Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, 132 Stat. 1253 (2018). A few days before those limits went into effect, though, Backpage.com was indicted and shut down under a preexisting, unrelated law. *See, e.g.*, ERIC GOLDMAN, INTERNET LAW: CASES AND MATERIALS 303–10 (2018).

First and Fourth Amendments and § 230 of the Communications Decency Act make it hard or impossible for government to demand cooperation from platforms. These legal constraints can sometimes be overcome through legislation or clever argument, but other times they reflect important policy objectives that cannot or should not be overcome.

Section 230, in particular, would be a major obstacle to efforts to force platforms to detect and prevent scams. Section 230 gives online platforms broad immunity from liability for user-posted content; with a few exceptions for things like intellectual property, that liability insulates platforms not only from money damages for distributing user-posted content, but also from prospective relief like court orders to take down content.[226] It's easy to see why some sort of immunity is necessary, since platforms could not operate at scale if they had to police every user post.[227] The same is true for advertising: platforms serve billions of ads every day, and asking them to exercise due diligence over each of those ads would be impossible.[228] Section 230 has been held, then, to apply even when

226. 47 U.S.C. § 230 (2012). For some of the most striking applications of § 230, see, for example, Fields v. Twitter, Inc., 217 F. Supp. 3d 1116, 1120–29 (N.D. Cal. 2016) (holding that Twitter could not be held liable for providing material support to terrorists for allowing them to use its service), *aff'd on other grounds*, 881 F.3d 739 (2018); Jones v. Dirty World Entm't Recordings LLC, 755 F.3d 398, 406–17 (6th Cir. 2014) (holding that the Dirty World website could not be held liable for publishing allegedly defamatory gossip submitted by users, even when it solicited the user submissions, refused to remove any, and added its own commentary); Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1173–77 (2009) (holding that defendant could not be held liable for including plaintiff's product in a list of alleged malware); Doe v. MySpace, Inc., 528 F.3d 413, 418–22 (5th Cir. 2008) (holding that MySpace could not be held liable for negligence when it allegedly failed to take reasonable precautions to prevent sexual predators from using the site to prey on minors); Blumenthal v. Drudge, 992 F. Supp. 44, 49–53 (D.D.C. 1998) (holding that AOL, which licensed and republished Matt Drudge's gossip column, could not be held liable for defamation allegedly contained in the column); Zeran v. Am. Online, Inc., 129 F.3d 327, 330–34 (4th Cir. 1997) (holding that AOL could not be liable for defamation when it repeatedly promised to delete posts falsely accusing Zeran of selling offensive shirts about the Oklahoma City bombing, but failed to do so); *see also* Eric Goldman, *The Ten Most Important Section 230 Rulings*, 20 TUL. J. TECH. & INTELL. PROP. 1, 2–9 (2017) (discussing how cases involving § 230 have built such an immunity); Eric Goldman & Jeff Kosseff, *Commemorating the 20th Anniversary of Internet Law's Most Important Judicial Decision*, RECORDER, (Nov. 10, 2017, 4:00 AM), https://www.law.com/therecorder/sites/therecorder/2017/11/10/commemorating-the-20th-anniversary-of-internet-laws-most-important-judicial-decision/ [https://perma.cc/R4WL-E9PW] (listing a collection of essays regarding the seminal case*, Zeran v. AOL*).

227. *See, e.g.*, JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET 60 (2019); Roger Allan Ford, *How the Supreme Court Ignored the Lesson of 'Zeran' and Screwed up Copyright Law on the Internet*, RECORDER, (Nov. 10, 2017, 12:45 AM) https://www.law.com/therecorder/sites/therecorder/2017/11/10/how-the-supreme-court-ignored-the-lesson-of-zeran-and-screwed-up-copyright-law-on-the-internet/ [https://perma.cc/U5E9-WZX5].

228. *See, e.g.*, Pamela Parker, *Google Bringing in More Than $100 Million Per Day Via AdWords*, SEARCH ENGINE LAND (Oct. 25, 2012, 1:55 PM), https://searchengineland.com/goo

platforms serve allegedly fraudulent ads,[229] and similar reasoning would apply to any government effort to get platforms to detect or prevent scams.

Amending § 230 would overcome the legal problem, but designing an effective amendment would be difficult. It would need to encourage platforms to develop and deploy scam-detection tools without punishing them for mistakes or failures if those tools don't catch every scam.[230] One option would be a regime that holds platforms liable only when they have actual notice of a scam. The similar notice-and-takedown provision in copyright law, though, has mostly failed.[231] It has failed to reduce the amount of infringing material distributed on the internet.[232] It has also led to the removal of noninfringing material, since platforms have mostly set up systems to automatically remove content when they get a notice of an alleged infringement, without evaluating the merits of the complaint.[233] Maybe overinclusion wouldn't be a substantial downside when it comes to ads, but many businesses are so dependent on online platforms and advertising that even small changes in Google's search algorithm can make or break them, so reducing the reliability of online advertising could have substantial downsides.[234]

Despite these difficulties, encouraging platforms to detect and prevent scams could be a plausible option. Between the technical obstacles to law-enforcement detection efforts and the legal

---

gle-bringing-in-100-millionday-via-adwords-says-study-137583 [https://perma.cc/VKX8-LJPY] (estimating, in 2012, that Google served more than thirty-one billion ads a day).

229. *See* Goddard v. Google, Inc., 640 F. Supp. 2d 1193, 1196–1201 (N.D. Cal. 2009) (holding that Google could not be held liable for serving allegedly fraudulent ads for mobile-phone services like ringtones).

230. *See, e.g.*, Mark A. Lemley, *Rationalizing Internet Safe Harbors*, J. TELECOMM. & HIGH TECH. L., Fall 2007, at 101, 110–18 (discussing the benefits and challenges of various internet safe harbors with regard to amending § 230).

231. *See* 17 U.S.C. § 512 (2012).

232. *See, e.g.*, BRUCE BOYDEN, CTR. FOR THE PROT. OF INTELLECTUAL PROP., THE FAILURE OF THE DMCA NOTICE AND TAKEDOWN SYSTEM: A TWENTIETH CENTURY SOLUTION TO A TWENTY-FIRST CENTURY PROBLEM 1 (2013), http://sls.gmu.edu/cpip/wp-content/uploads/sites/31/2013/08/Bruce-Boyden-The-Failure-of-the-DMCA-Notice-and-Takedown-System1.pdf [https://perma.cc/E79N-Q4PP].

233. *See, e.g.*, Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, HARV. J.L. & TECH., Fall 2010, at 171, 172–75. *But see* Annemarie Bridy, *Is Online Copyright Enforcement Scalable?*, 13 VAND. J. ENT. & TECH. L. 695, 698, 712–14 (2011) (arguing that the DMCA "has proven to be remarkably scalable for enforcing copyrights in hosted content but has altogether failed to scale in the context of [peer-to-peer] file sharing").

234. *See, e.g.*, Neal Ungerleider, *What Google Search Algorithm Changes Do to the Internet*, FAST COMPANY (May 21, 2014), https://www.fastcompany.com/3030848/what-google-search-algorithm-changes-do-to-the-internet [https://perma.cc/R5RN-LW3E].

obstacles to platform efforts, the legal obstacles are likely easier to overcome.[235] Platforms may be wary of handing over user information to law-enforcement agencies or giving agencies powers that they could abuse, but they also don't want their platforms to be overrun by scams. They might be susceptible, then, to soft-power efforts to encourage them to develop and deploy scam-detection tools.

But the incentive problems are real. Remember Uber's fairly successful efforts to detect scams that rip off the company, discussed above?[236] Uber is just as heavily plagued by scams that rip off passengers—yet the company has seemingly done much less to combat them.[237] The difference is obvious: One set of scams harms the company directly, while the other just harms customers. Even if the latter winds up hurting the company's image or customer satisfaction, the effect is indirect and ambiguous, and so much easier to ignore. Likewise, it is much easier for targeting platforms to ignore scams that rip off their customers compared to those that rip off the platforms.

V. IMPLICATIONS

The problem of data scams is one with its roots in aggregated personal information, but it is not a classic privacy problem. Nothing about scammers' use of targeting platforms leads to any

235. Though not trivial. For more on the difficulties of using financial incentives to encourage platforms to police user behavior see Annemarie Bridy, *Internet Payment Blockades*, 67 FLA. L. REV. 1523, 1554–67 (2015); Jake Linford, Response, *Private Ordering Under Threat of Regulation*, 67 FLA. L. REV. F. 298, 301–12 (2016).

236. *See supra* notes 196–203 and accompanying text.

237. The latest example is "vomit fraud," which occurs when a driver falsely reports to Uber that a passenger vomited in the car and Uber charges the passenger a clean-up fee. *See, e.g.*, Catalina Ruiz Parra, *It's Called Vomit Fraud. And It Could Make Your Uber Trip Really Expensive*, MIAMI HERALD (July 22, 2018, 8:40 AM), https://www.miamiherald.com/news/business/article215299675.html. Passengers frequently report that it takes many e-mails to get Uber to reverse the charge, or that Uber refuses to do so. *Id.* This isn't the only scam drivers pull on passengers. For others, see for example, Angelina Aucello, *I Was Victim of an Increasingly-Popular Uber Scam*, ANGELINA TRAVELS (July 13, 2015), https://angelinatravels.boardingarea.com/2015/07/13/i-was-victim-of-an-increasingly-popular-uber-scam/ [https://perma.cc/G5J9-8XN5] (describing a scam in which a driver falsely told Uber there were too many passengers in the car, causing the company to upgrade the fare from Uber X to the more-expensive Uber XL); Samuel Gibbs, *Uber's 'Ghost Drivers' Scaring Passengers out of Rides and Money*, GUARDIAN (Sept. 22, 2016, 11:51 AM), https://www.theguardian.com/technology/2016/sep/22/uber-ghost-drivers-zombie-profile-pictures [https://perma.cc/7U3T-VDL9] (describing a scam in which a driver uses a disturbing profile photo, hoping to scare off passengers and pocket cancelation fees). Blog posts and friendly journalistic features describing Uber's sophisticated efforts to eliminate these scams are rather scarcer than with the scams targeting Uber itself. For example, a Google search of the matter returns only one journalistic feature relating to Uber's efforts. *See also* Ng, *supra* note 199 (discussing the efforts Uber has made using machine-learning tools to reduce scams on the platform).

of the classic privacy losses: no information about targeted consumers or scam victims is necessarily revealed to scammers or the public. In some cases, information is revealed—for instance, when a user clicked on the "Dinner with Trump" ad and contributed to the American Horizons PAC, the PAC got the contributor's name, employment information, and so forth as required by federal election law—but it's also possible that a scam might not reveal anything. A scam that installed malware on a user's computer to mine bitcoins or send spam e-mails, for instance, or that spread false information or sold digital downloads, might not reveal any personal information.

This feature of data scams is not unique. Instead, they may represent an instance of a broader phenomenon of nonprivacy problems that nevertheless stem from the mass aggregation of personal information. By compiling personal information into large datasets and making it easy and cheap to use that information for targeting, platforms create a set of structural externalities, casting doubt on the social benefits of targeting platforms. While some of these effects have been recognized by scholars and policy makers, others have not; nor has that recognition changed the basic view that targeting platforms represent a tradeoff between efficiency and privacy. These externalities fall into two broad categories: effects on the consumer marketplace and effects on the democratic system.

The Consumer Marketplace. Targeting platforms affect the marketplace by giving advertisers and sellers information about individual consumers, which has two basic effects. First, it changes the bargaining positions of consumers and producers by reducing the information asymmetry between them or even creating new asymmetries in favor of producers. When a producer knows that a particular consumer is loyal to a particular brand, for instance, it can use that information to charge a higher price; when a producer knows that a consumer is focused on a particular feature, it can highlight that feature. Even when transactions represent voluntary, arms-length exchanges between rational actors, then, the effect of targeting is to boost producers' bargaining power through tools like price discrimination. This may not necessarily be a bad thing—the economics of price discrimination are complicated, though there are reasons to think that it often creates wealth[238]—but it undoubtedly changes how

238. *See, e.g.*, Einer Elhauge, *Tying, Bundled Discounts, and the Death of the Single Monopoly Profit Theory*, 123 HARV. L. REV. 397, 426–42 (2009); Barry Nalebuff, Response, *Price Discrimination and Welfare*, 5 COMPETITION POL'Y INT'L 221, 229–30 (2009). For just

consumer and producer surplus are distributed, effecting a systematic wealth transfer from consumers to producers. Moreover, since producers are likely wealthier to begin with, this should be expected to increase wealth inequality. That won't matter to some, but it matters for adherents to metrics of social welfare that go beyond pure utilitarianism.

Second, targeting also makes it easier for sellers to engage in transactions that might *not* represent voluntary, arms-length exchanges between rational actors. Scams are an example of this, but there are other ways that sellers can take advantage of data and targeting to conduct what Ryan Calo calls "digital market manipulation."[239] By using targeting platforms to identify individual cognitive biases specific to different people, for instance, a seller might know exactly how to persuade someone to buy the most profitable item in a category. Maybe someone is more willing to overpay or buy pointless goods in the afternoon, taking a break at work. Maybe they're more willing to do so on Tuesdays in May and July, for reasons no one can explain.[240] Regardless, this information can be exploited. Companies have always tried to identify and exploit cognitive biases, but it is far more powerful if they can identify each person's individual biases, further shifting the relative bargaining power of consumers and producers.[241]

The Democratic System. Targeting platforms also affect the democratic process in ways that scholars and policy makers are increasingly grappling with. Much has been reported about ways that Russia used Facebook and Twitter to affect the 2016 presidential election,[242] but it goes beyond that. More basic

---

a few of the foundational works in the literature, see generally, for example, LOUIS PHLIPS, THE ECONOMICS OF PRICE DISCRIMINATION (1983) (offering a theoretical and unified explanation of how prices are determined in practice); GEORGE J. STIGLER, THE THEORY OF PRICE 210–13 (4th ed. 1987) (providing an overview of the varieties of monopoly pricing); JEAN TIROLE, THE THEORY OF INDUSTRIAL ORGANIZATION 133–34 (1988) (describing the modern theory of monopoly and intertemporal price discrimination); Hal R. Varian, *Price Discrimination*, *in* 1 HANDBOOK OF INDUSTRIAL ORGANIZATION 597 (Richard Schmalensee & Robert D. Willig eds., 1989) (providing an overview of the theory of price discrimination and its applications).

239. *See* Calo, *supra* note 6, at 995, 1003–18.

240. *Cf.* Chris Anderson, *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*, WIRED (June 23, 2008, 12:00 PM), https://www.wired.com/2008/06/pb-theory/ [https://perma.cc/9CNH-QNLK].

241. *See* Calo, *supra* note 6, at 1007–12. This "mass production of bias" is just one of three mechanisms of manipulation that Calo discusses. *See id.* at 1003–18.

242. *See, e.g.*, Tony Romm & Kurt Wagner, *Facebook Says 126 Million People in the U.S. May Have Seen Posts Produced by Russian-Government-Backed Agents*, VOX (Oct. 30, 2017, 6:00 PM), https://www.recode.net/2017/10/30/16571598/read-full-testimony-facebook-twitter-google-congress-russia-election-fake-news [https://perma.cc/S4ZD-Y62Z]; Tony Romm, *10 Million People Saw Russian Ads on Facebook Around the 2016 Presidential*

questions of democratic legitimacy and accountability arise when candidates use targeting platforms.[243] Democratic legitimacy depends on voters being informed about the policies supported by candidates for elected office and having the opportunity to deliberate about those policies and ratify them through fair and free elections.[244] Targeting lets candidates present different versions of themselves to different voters—up to and including different positions on the same issue.[245] When this happens, have voters meaningfully ratified the positions later taken by the officeholder? This problem doesn't necessarily go away when one has taken office; elected officials have also learned the value of telling different people different things about what they're doing in office.[246] If they work—a prospect that seems increasingly likely in an era of eroding trust in the news media[247]—then such ads would help avoid accountability even for one's core campaign positions.

The existence of these externalities suggests that the case for regulating—maybe even banning—targeting platforms and technologies is stronger than it seems. Regulation is most readily justified when it addresses a market failure, and externalities are

---

Election, VOX (Oct. 2, 2017, 6:43 PM), https://www.recode.net/2017/10/2/16405900/russian-advertisements-facebook-2016-us-presidential-election-trump-clinton [https://perma.cc/JJC9-DLF2]; Scott Shane, *To Sway Vote, Russia Used Army of Fake Americans*, N.Y. TIMES, Sept. 8, 2017, at A1, A10–A11; *see also* Dipayan Ghosh & Ben Scott, *Russia's Election Interference is Digital Marketing 101*, ATLANTIC (Feb. 19, 2018), https://www.theatlantic.com/international/archive/2018/02/russia-trump-election-facebook-twitter-advertising/553676/ [https://perma.cc/X9DX-6SEM] (discussing the unchecked market power of social media with regard to Russia's meddling in the U.S. election).

243. *See, e.g.*, HERSH, *supra* note 54, at 205–13.

244. *See, e.g.*, Robert Post, Commentary, *Regulating Election Speech Under the First Amendment*, 77 TEX. L. REV. 1837, 1841–42 (1999); Seyla Benhabib, *Toward a Deliberative Model of Democratic Legitimacy*, *in* DEMOCRACY AND DIFFERENCE: CONTESTING THE BOUNDARIES OF THE POLITICAL 67, 69 (Seyla Benhabib ed., 1996); Joshua A. Cohen, *Deliberation and Democratic Legitimacy*, *in* THE GOOD POLITY: NORMATIVE ANALYSIS OF THE STATE 17, 18–19 (Alan Hamlin & Philip Pettit eds., 1989).

245. *See, e.g.*, ELI PARISER, THE FILTER BUBBLE: HOW THE NEW PERSONALIZED WEB IS CHANGING WHAT WE READ AND HOW WE THINK 152–56 (2012).

246. *See, e.g.*, Craig Silverman, *Trump Is Using Targeted Facebook Ads to Reassure Supporters He Will Build the Border Wall*, BUZZFEED NEWS (Sept. 20, 2017, 9:10 AM), https://www.buzzfeednews.com/article/craigsilverman/trump-is-using-targeted-facebook-ads-to-reassure-supporters [https://perma.cc/P84P-2SRF] (reporting that President Trump ran "dark" Facebook ads, targeted at supporters and invisible to others, "to reassure supporters . . . after his recent public comments caused many to question whether he would keep his promise" to build a wall along the southern border of the United States).

247. *See, e.g.*, *American Views: Trust, Media and Democracy*, KNIGHT FOUND. (Jan. 15, 2018), https://knightfoundation.org/reports/american-views-trust-media-and-democracy [https://perma.cc/6EWH-3RF3] (reporting, based on survey results, that "Americans' perceptions of the news media are generally negative, and their perceptions of bias have grown considerably from a generation ago").

a classic example.[248] Platforms are able to monetize targeting without incurring all of its costs because these effects on the consumer marketplace and the democratic system are felt by the broader public.[249] If a targeting platform systematically impoverishes consumers or harms democracy, well, that's not the platform's problem. Yet, at least in the United States, targeting platforms are essentially unregulated. The major exception is the FTC's settlement-driven body of law defining deceptive and unfair trade practices,[250] but the Commission hasn't applied that law to the basic practice of targeted advertising.

Maybe it should. Under the FTC Act, an unfair trade practice is one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[251] This is not an unreasonable description of these systemic effects of targeting platforms, even setting aside the political effects. Targeting injures consumers when it facilitates manipulation, enables scams, and reduces consumers' bargaining power. Though there are countervailing benefits to consumers, like funding free content or providing them relevant information about products and services, it is far from clear that these benefits are large enough to offset the costs. Advertising funded free content well before targeting platforms were possible, so the real question is not whether targeted advertising funds free content, but what the size of the incremental improvement is—and there are reasons to think it is small.[252] So the naïve solution of just banning targeted advertising may have more to recommend it than it seems.[253]

Still, targeting probably isn't going anywhere anytime soon. In a world of second-best solutions, then, it is probably slightly easier to overcome platforms' incentive problems than to overcome agencies' expertise problems, so giving platform operators incentives to structure their platforms to make it easier to detect and prevent scams could be a useful intervention. Scams are not, however, a problem that is likely amenable to a single cure-all.

248. *See, e.g.*, THOMAS A. LAMBERT, HOW TO REGULATE: A GUIDE FOR POLICYMAKERS 22–59 (2017).

249. It's possible that unusually high-profile platforms like Facebook and Google do bear some of these costs, since many of the ads they serve are seen on their own pages and since privacy problems on each platform have been well covered by the press. Other, less-famous platforms should bear few or none of these costs.

250. *See* Solove & Hartzog, *supra* note 88; *supra* notes 84–98 and accompanying text.

251. 15 U.S.C. § 45(n) (2012).

252. *See supra* note 65 and accompanying text.

253. *See supra* notes 187–88 and accompanying text.

Different approaches—better incentives for platforms, better tools for agencies, and more resources for investigating and prosecuting scammers—may need to be combined.

VI. CONCLUSION

Platforms like Google and Facebook make it easier and cheaper to target customers, but they also make it easier and cheaper to scam those customers. Platforms facilitate these data scams by making three things easier for scammers: finding the most promising victims, hiding from authorities, and developing the most effective scams. As more and more social behavior moves online, the result could be that vulnerable individuals and groups are increasingly victimized by malicious actors.

Data scams are a problem rooted in technology, which means they may be amenable to a technological solution. One such solution would be to use the same analytics tools that enable targeting in the first place to detect and prevent scams, though efforts to encourage platforms and law-enforcement agencies to do so would have to overcome significant difficulties. Still, targeting isn't going anywhere anytime soon, so giving operators incentives to structure their platforms to make it easier to detect and prevent scams may be a promising solution.

At the same time, data scams are a curious phenomenon because they stem from the mass aggregation of personal information and yet lead to harms that are not classic privacy harms. They are not unique in this way; instead, they may represent a broader class of ways that data aggregation can hurt the consumer marketplace and democratic system. If so, then more aggressive solutions, like regulation or even a targeting ban, may need further consideration.