THE ANTITRUST CASE AGAINST FACEBOOK

A MONOPOLIST'S JOURNEY TOWARDS PERVASIVE SURVEILLANCE

IN SPITE OF CONSUMERS' PREFERENCE FOR PRIVACY

Dina Srinivasan*

This version of *The Antitrust Case Against Facebook* is a draft version. The final version of this article is forthcoming and will be published in January 2019 in the *Berkeley Business Law Journal* Vol. 16, Issue 1.

*This article arose from my personal observations as an entrepreneur and executive in the digital advertising industry. I am grateful to Fiona Scott Morton, Alvin Klevorick, Michael Kades, Charles Reichmann, and Robert Litan for conversation and feedback at various stages. I extend a warm thank you to George Priest for inspiring an interest in antitrust years ago. I would also like to thank the editors at the University of California Berkley Business Law Journal for their careful edits, the journalists and researchers for uncovering and reporting on the facts relied on in this paper, and the University of Chicago for hosting the 2018 Antitrust and Competition Conference: Digital Platforms and Concentration. No party provided to me any direct or indirect financial support during the writing of this article.

CONTENTS

ABSTRACT

The Facebook, Inc. ("Facebook") social network, this era's new communications service, plays an important role in the lives of 2+ billion people across the world. Though the market was highly competitive in the beginning, it has since consolidated in Facebook's favor. Today, using Facebook means to accept a product linked to broad-scale commercial surveillance—a paradox in a democracy. This Paper argues that Facebook's ability to extract this qualitative exchange from consumers is merely this titan's form of monopoly rents. The history of early competition, Facebook's market entry, and Facebook's subsequent rise tells the story of Facebook's monopoly power. However, the history which elucidates this firm's dominance also presents a story of anticompetitive conduct. Facebook's pattern of false statements and misleading conduct induced consumers to trust and choose Facebook, to the detriment of market competitors and consumers' own welfare.

INTRODUCTION

Social networks, considered electronic communication service providers,[1] have become a primary way that American consumers communicate.[2] Facebook is the reigning platform, not only in the lives of Americans, but in the lives of 2.2 billion people worldwide.[3] Though the social network market was highly competitive in the beginning,[4] the market has since consolidated in Facebook's favor. Consumers effectively face a singular choice—use Facebook and submit to the quality and stipulations of Facebook's product or forgo all use of the only social network used by most of their friends, family, and acquaintances.

When Facebook entered the market, the consumer's privacy was paramount. The company prioritized privacy, as did its users—many of whom chose the platform over others due to Facebook's avowed commitment to preserving their privacy. Today, however, accepting Facebook's policies in order to use its service means accepting broad-scale commercial surveillance.

---

[1] Various federal laws regulate electronic communication service providers, including the Electronic Communications Privacy Act, 18 U.S.C.§ 2510 (ECPA), Titles I and II of the ECPA specifically (the Wiretap Act, 18 U.S.C. § 2510-2521, the Stored Communications Act, 18 U.S.C. § 2701-2711 (SCA)), and the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 (2008). Several courts have considered Facebook's duties and lack thereof under these statutes. *See, e.g.*, Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010) (quashing subpoena portions for private messages from Facebook and MySpace because the SCA prohibits production). S*ee also In re* Facebook Privacy Litig., 791 F. Supp. 2d 705, 711-13 (N.D. Cal. 2011); *In re* Facebook Internet Tracking Litig., 140 F. Supp. 3d 922 (2015). For an overview of relevant cases, *see* IAN C. BALLON, *Cyber Boot Camp: Data Security at the Intersection of Law and Business*, *in* E-COMMERCE AND INTERNET LAW: A LEGAL TREATISE WITH FORMS (2d ed. 2016), http://legacy.callawyer.com/wp-content/uploads/2016/05/2017-01-12-DJ-LA-CyberSecurityBootcamp-aPrivacyLit.pdf.

[2] *See generally* Frank Newport, *The New Era of Communication Among Americans*, GALLUP.COM (Nov. 10, 2014), https://news.gallup.com/poll/179288/new-era-communication-americans.aspx.

[3] *Company Info,* NEWSROOM.FB.COM (July 20, 2018), https://newsroom.fb.com/company-info/.

[4] In 2007, there were hundreds of social networks, including competitive offerings from Google, Yahoo, and of course, MySpace. *See generally* Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J, OF COMPUTER-MEDIATED COMM. 210 (2007).

Facebook knows consumers' identities by virtue of its position as this century's new communications network and leverages this knowledge to build dossiers on consumers that are unrivaled in the private market. For Max Schrems, then a 23-year-old law student who used European law to petition Facebook for a copy of his data, his Facebook file as of 2011 was 1,200 pages long.[5] That was before Facebook started monitoring and recording users' activities not just on the singular Facebook domain, but on millions of independently owned websites and mobile applications.[6] Facebook's surveillance apparatus captures what people read, shop for, and even think,[7] online. For Americans that use an Android phone, Facebook apparently also scrapes a record of a user's cellular phone calls—effectively rendering use of the Facebook social network

[5] Max Schrems, now a leading advocate at the intersection of user privacy and Big Tech, initially filed claims against Facebook with the Irish Data Protection Commissioner (IDPC) for violations of European data protection law. For the files Schrems originally obtained from Facebook, *see Facebook's Data Pool,* FACEBOOK.COM, http://europe-v-facebook.org/EN/Data_Pool/data_pool.html (last visited July 27, 2018). Following the revelations of whistleblower Edward Snowden, and the specific leak of National Security Agency (NSA) Prism slides claiming Facebook was supplying the NSA with copies of user communications and other social network data, Schrems filed an additional complaint with the IDPC alleging that the transfer of his data from the E.U. to U.S. jurisdiction violated the European Union Directive on Data Protection (Directive 95/46/EC), which as of May 25, 2018, has been replaced with the General Data Protection Regulation (GDPR). The suit eventually caused an international crisis when it resulted in the downfall of the Safe Harbour framework for E.U.-U.S. corporate data transfers. *See Maximillian Schrems v. Digital Rights Ireland Ltd.* [2015] C-362/14 (H. Ct.) (Ir.). For coverage of the Snowden leaks, Prism, and Facebook's alleged participation in Prism, *see* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data From Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.8e7f22acf1c0; Glen Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/us-techgiants-nsa-data [http://perma.cc/G4AD-DA88]. For the leaked NSA PowerPoint slides describing Prism and Facebook's involvement with Prism, *see PRISM Overview Powerpoint Slides*, ACLU.ORG (April 2013), https://www.aclu.org/other/prism-overview-powerpoint-slides.

[6] Facebook can track consumer behavior on the millions of independent websites and apps that use any of Facebook's business products (Like buttons, Logins, conversion tracking pixels, software development kit, et al.). The Facebook Like buttons alone appear on nearly 3 million websites. *Websites using Facebook Like Button*, BUILTWITH.COM (2018), https://trends.builtwith.com/websitelist/Facebook-Like-Button.

[7] Facebook has collected the text users type, but then delete, into status updates, timeline posts, and comments, before hitting an enter button. See Sauvik Das & Adam Kramer, *Self-Censorship on Facebook*, PROCEEDINGS OF THE SEVENTH INTERNATIONAL AAAI CONF. ON WEBLOGS AND SOCIAL MEDIA, https://www.aaai.org/ocs/index.php/ICWSM/ICWSM13/paper/viewFile/6093/6350. It is unclear whether Facebook's privacy policy at the time permitted Facebook to do this. *See generally* Jennifer Golbeck, *On Second Thought …*, SLATE (Dec. 13, 2013), https://slate.com/technology/2013/12/facebook-self-censorship-what-happens-to-the-posts-you-dont-publish.html.

app to the equivalent of having a pen register on one's device.[8] Surveillance translates to influence,[9] on many levels. As we learned recently, information gathered thereby can be misappropriated to influence political elections.[10]

Facebook also sells advertising to marketers. In the digital advertising market, the ability to conduct unprecedented commercial surveillance is a bedrock of Facebook's current revenues and profits. Facebook generates nearly all of its revenues from the sale of advertising,[11] and the prices of ads sold today directly correlate with data derived from tracking consumers.[12] Facebook

---

[8] Tom Warren, *Facebook Has Been Collecting Call History and SMS Data From Android Devices*, THE VERGE (Mar. 25, 2018), https://www.theverge.com/2018/3/25/17160944/facebook-call-history-sms-data-collection-android; Alex Hern, *Facebook Logs SMS and Calls, Users Find as They Delete Accounts*, THE GUARDIAN (Mar. 26, 2018), https://www.theguardian.com/technology/2018/mar/25/facebook-logs-texts-and-calls-users-find-as-they-delete-accounts-cambridge-analytica.

[9] Data derived from surveillance is used to create psychographic profiles of individual consumers. Whereas demographic data refers to the variables of age, income, and education, psychographic data refers to the broader range of data sets that reflect a consumer's personality, opinions, attitudes, interests, values, past activity, and general lifestyle. Psychographic data is used by companies to determine which piece of content, advertisement, or even price, to display to a particular consumer, in an attempt to influence consumer outcome. For a study of how psychographically targeted advertising changes the outcome of consumer behavior, see, e.g., S. C. Matz, M. Kosinski, G. Nave, & D. J. Stillwell, *Psychological Targeting as an Effective Approach to Digital Mass Persuasion*, PNAS (Nov. 2017), http://www.pnas.org/content/early/2017/11/07/1710966114.short. For background on psychographics, see generally, William D. Wells, *Psychographics: A Critical Review*, 12 J. OF MARKETING RES. 196 (1975), www.jstor.org/stable/3150443.

[10] After the conclusion of the 2016 U.S. presidential election, Facebook disclosed to congressional investigators that it had sold to a Russian company, Internet Research Agency (IRA), ads which psychographically targeted American voters, and that up to approximately 126 million people could have been exposed to such ads. *See* Dylan Byers, *Facebook Estimates 126 Million People Were Served Content from Russia-linked Pages*, CNN.COM (Oct. 31, 2017), https://money.cnn.com/2017/10/30/media/russia-facebook-126-million-users/index.html; *Facebook, Google and Twitter Executives on Russian Disinformation*, C-SPAN.ORG (Oct. 31, 2017), https://www.c-span.org/video/?436454-1/facebook-google-twitter-executives-testify-russia-election-ads. In March 2018, it was revealed that Facebook data, including Like data, on more than 87 million users was misappropriated and used by political consulting firm Cambridge Analytica to psychographically target voters during the presidential race. For The *New York Times* story that cascaded response from U.S. and British lawmakers (in Britain, for alleged interference in the "Brexit" campaign) and resulted eventually in Facebook founder and chief executive officer Mark Zuckerberg's live testimony before Congress, *see* Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (March 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[11] Advertising revenues contributed 98+% of Facebook's 40+ billion in revenues in 2017. FACEBOOK INC., Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 (Form 10-K) (2017).

[12] Consider comments of Dave Wehner, the chief financial officer of Facebook, on Facebook's Q2 earnings call, with respect to how privacy (or, a reduction in user data) is inversely correlated with Facebook revenues. *Facebook Inc. Q2 2018 Earnings Conference Call*, INVESTOR.FACEBOOK.COM (July 25, 2018), https://s21.q4cdn.com/399680738/files/doc_financials/2018/Q2/Q218-earnings-call-transcript [hereinafter "*Facebook Q2 Earnings*"].

leverages information it knows about users to sell more impression-targeted ads and more action-based ads.[13] Facebook then uses this capability to sell advertising on behalf of other market participants—like Hearst, The *Washington Post*, or Time, Inc.[14] Facebook's power here is so absolute that the duopoly of Facebook and Google accounts for 90-99% of year-over-year growth in the U.S. digital advertising market.[15]

But in a country anchored by democratic values and fear of tyranny derived from breaching individual civil liberties, why does the free market today offer no real alternative to the exchange of free use of social media for pervasive surveillance? Why is it that thousands of Facebook competitors on the advertising side—traditional publishers of content, such as magazines and newspapers—also coordinate *with* Facebook to allow Facebook to watch and monitor their own customers? Why must consumers consent to identical Facebook terms in the privacy policies of other sellers of digital advertising? Does the free market today reflect consumer welfare, or does it enable a monopolist to offer inferior quality products by coordinating with other market participants?

---

[13] For example, if one advertising company has 5,000 data points per consumer, including the data points for age and propensity for depression, then that company can fulfill more orders for a campaign targeted to 20-year-olds that read about suicide than can another company that reaches the same audience but does not possess said user data points. I acknowledge that tailored advertising can reflect either a positive or negative product evolution for consumers, and I do not wish to enter this parallel debate. Rather, I wish to focus on the successful operation, or lack thereof, of consumer preference and choice in the market—a paramount concern in economics.

[14] Facebook sells the advertising inventory of companies that compete with Facebook on the advertising side of the market via a program called the Facebook Audience Network (FAN). *Facebook for Developers*, FACEBOOK.COM (2018), https://developers.facebook.com/products/audience-network.

[15] In a note to clients on 4/26/17, respected industry analyst Brian Wieser calculated that Facebook and Google accounted for 77% of the industry's gross revenues in 2016, 99% of the growth in the U.S. digital ad market, and that "the average growth rate for every other company in the sector was close to 0." Facebook alone accounted for 77% of the industry's year-over-year growth. *See* Alex Heath, *Facebook and Google Completely Dominate the Digital Ad Industry*, BUSINESSINSIDER.COM (April 26, 2017), http://www.businessinsider.com/facebook-and-google-dominate-ad-industry-with-a-combined-99-of-growth-2017-4. Wieser estimated that Facebook and Google contributed 90% to the U.S. digital ad market's growth in 2018. Sarah Sluis, *Digital Ad Market Soars to $88 Billion, Facebook and Google Contribute 90% of Growth*, ADEXCHANGER.COM (May 10, 2018), https://adexchanger.com/online-advertising/digital-ad-market-soars-to-88-billion-facebook-and-google-contribute-90-of-growth/.

Colloquially, and in the press, Facebook is a monopoly.[16] Members of Congress, reporters, academics, and even initial founders of Facebook are speaking of Facebook's monopoly power and questioning the need for regulation.[17] However, from an academic standpoint, the intellectual and legal case of monopoly has not yet been made,[18] perhaps due to the nature of Facebook's product being still "free" to the consumer. The fact that the product is free falsely diverts attention from what antitrust policymakers and economists are most comfortable paying attention to: price. Nevertheless, antitrust law and economics concern quality inasmuch as they do price. As I will argue in this Paper, Facebook is a monopolist, and what Facebook extracts overtly from consumers today, from a quality perspective, is a direct function of Facebook's monopoly power.

---

[16] *See, e.g.*, recent dialogue between Lindsey Graham (R-SC) and Facebook founder and chief executive officer Mark Zuckerberg (Graham pressed Zuckerberg to identity competitors in the private market), and between House judiciary committee chairman Bob Goodlatte (R-Va.) and Facebook vice president of global policy management Monika Bickert (Goodlatte asked Bickert about the lack of competition Facebook faces). *Hearing on Facebook Congressional Hearing Before the Committee on Energy and Commerce*, 115th Cong. (April 2018). For a transcript of the hearing, see *Transcript of Zuckerberg's Appearance Before House Committee*, WASH. POST (April 11, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/transcript-of-zuckerbergs-appearance-before-house-committee/?utm_term=.c12ab1475612. Also consider recent coverage in leading news publications, including: David J. Lynch, *Big Tech and Amazon: Too Powerful to Break Up?* FINANCIAL TIMES (Oct. 29, 2017), https://www.ft.com/content/e5bf87b4-b3e5-11e7-aa26-bb002965bce8; Christopher Mims, *Tech's Titans Tiptoe Toward Monopoly*, WALL STREET J. (May 31, 2018), https://www.wsj.com/articles/techs-titans-tiptoe-toward-monopoly-1527783845; Jonathan Taplin, *Forget AT&T. The Real Monopolies Are Google and Facebook*, N.Y. TIMES (Dec. 13, 2016), https://www.nytimes.com/2016/12/13/opinion/forget-att-the-real-monopolies-are-google-and-facebook.html; Micah L. Sifry, *In Facebook We Antitrust*, THENATION.COM (Oct. 12, 2017), https://www.thenation.com/article/in-facebook-we-antitrust/; Barry C. Lynn, *America's Monopolies Are Holding Back the Economy*, THE ATLANTIC (Feb. 22, 2017), https://www.theatlantic.com/business/archive/2017/02/antimonopoly-big-business/514358/.

[17] *Hearing on Facebook*, *supra* note 16.

[18] In the absence of clear rationale for how to interpret the paradoxes of Big Tech, there emerges a parallel push to reconsider antitrust law's coupling with economic rationale. *See, e.g.*, Lina Khan, *The New Brandeis Movement: America's Antimonopoly Debate*, 9 J. OF EUR. COMPETITION L. & PRACTICE 131 (2018), https://doi.org/10.1093/jeclap/lpy020 (referring to the movement as the "New Brandeis School," which urges that antitrust regulation should focus not only on consumer welfare but also the structure of markets to avoid mere concentrations of economic power). For coverage of the debate in the wider media, *see* Lynch, *supra* note 16. Others argue that economic thinking merely needs to be stretched to understand the 21st century's modern economy market problems. *See generally* Jonathan B. Baker, Jonathan Sallet & Fiona Scott Morton, *Introduction: Unlocking Antitrust Enforcement*, 127 YALE L.J. 1916 (2018).

The fact that the dominant player in the market conducts wide-scale commercial surveillance begs a question—how *did* the market get here? This Paper first explores this question by revisiting the rich record of the market's history. In so doing, I conclude that Facebook's ability to monitor and record consumers' digital activity reflects Facebook's ability to extract monopoly rents in the social media market. In Part I, I revisit the history of social networking and discuss how privacy was once a crucial promise made to secure a competitive advantage. Facebook foreclosed competition in a contested market with superior representations of protecting consumer privacy, including the specific promise not to track and monitor consumers' digital footprints.[19]

For a decade, the competitive market then enjoined Facebook's ability to initiate commercial surveillance. Facebook tried to renege on its promise not to track users in 2007, and again in 2010, but the market was competitive enough with adequate consumer choice to thwart Facebook's attempts.[20] Only after an historic public offering, the acquisition of over a billion users, and the exit of competitors, was Facebook finally able to add the condition of surveillance to its mandatory terms.[21] In Part II, I argue that this pattern of events reflects Facebook's monopoly power.

Part III argues that the circumstantial, or structural, evidence of Facebook's market dominance also explains Facebook's monopolistic power exhibited today. On the one hand, Facebook is a market in and of itself. Ninety-nine percent of adults in the U.S. that use social media use Facebook.[22] The reason for this is that Facebook is a "closed" communications network and users must join simply to access the network. Not all social networks are closed—LinkedIn, for example, disseminates user communications across its own network but also

[19] *See infra* note 42, FACEBOOK PRIVACY POLICY (2004).
[20] *Infra* Parts II A, II B.
[21] *See infra* Part II C.
[22] *See infra* Part III.

Twitter. But, Facebook, with a hold on the market and greatest number of users, declines the path of interconnection, or inter-operability. Consumers cannot forgo Facebook, in much the same way an earlier generation was beholden in the early 20th century to another communications behemoth, AT&T— another company that leveraged a closed-network approach to protect market share and foreclose competition in the telephone network market.[23] However, even if one does include other social networks as part of a relevant market, Facebook still dominates with over 80% of total consumer time spent across various social networks.

The story of Facebook's market entry, and the evolution of its commercial surveillance, raises another relevant question under antitrust law. Under Section 2 of the Sherman Act, [24] this country's antitrust statute, it is illegal for a company to acquire monopoly power by engaging in conduct outside the bounds of "competition on the merits."[25] Facebook engaged in a decade-long pattern of false statements and misleading conduct that may have induced users to trust and choose Facebook over alternatives in the market. Facebook also thereby secured the coordination of independent publishers and other businesses while perpetuating the belief that Facebook did not and would not leverage their coordination for surveillance. Facebook's conduct may have artificially shifted the demand curve for the Facebook social network to the right, effectively accelerating the direct network effects that would lock in Facebook and foreclose competition. Part IV explores Facebook's pattern of conduct and argues that it was anticompetitive.[26]

---

[23] Richard Gabel, *The Early Competitive Era in Telephone Communication, 1893-1920*, 34 LAW AND CONTEMPORARY PROBLEMS 340, 341 (1969) https://www.jstor.org/stable/pdf/1191094.pdf?refreqid=excelsior%3Ae9908dd1ed4a18092d06284ea77baf42.

[24] 15 U.S.C. § 2 (2000).

[25] United States v. Microsoft Corp., 253 F.3d 34 (D.C. Cir. 2001) (finding Microsoft conduct outside the scope of "competition on the merits" to be anticompetitive).

[26] Misleading conduct is of particular concern in markets with direct network effects. *See generally* PHILLIP E. AREEDA & HERBERT HOVENKAMP, FUNDAMENTALS OF ANTITRUST LAW § 350 (4th Ed. 2015) (Areeda and Hovenkamp explain that a "monopolist's misrepresentations encouraging the purchase of its product can fit [the] general test for an exclusionary practice when the impact on rivals is significant; deception of buyers can impede the opportunities of rivals."). *See also* Speech delivered by Carl Shapiro before the A.L.I. and A.B.A., 6 (Jan. 25, 1996), http://www.justice.gov/atr/public/speeches/0593.pdf (calling for heightened scrutiny of company behavior in

In digital markets where consumers do not pay a price, antitrust enforcement must become comfortable with a paradigm that focuses on quality. Never before have we had to grapple with one of the most valuable companies in the world, a half trillion-dollar market cap company,[27] that provides important communications services to over 2 billion consumers but charges no price. Policymakers and antitrust enforcers today can refer to the record in order to understand the consumer valuing privacy while still ceding control over their personal data, the flawed market structure that allows for the perpetuation of present circumstances, and the remedy which can restore competition in communications markets.

I. PRIVACY WAS ONCE A CRUCIAL FORM OF COMPETITION

To appreciate Facebook's monopoly power in the social network market today, one must begin by revisiting the story of Facebook's rise. In the beginning, the social media market reflected the type of competitive markets one reads about in textbooks. Dozens of companies competed furiously in an attempt to win market share. In a market where all competing products were priced at zero, startups competed not on price, but on quality. Privacy levels quickly emerged as an important quality attribute.[28]

Facebook was not the world's first major social network—MySpace was. In fact, in the market's early years, MySpace dominated. Founded in 2003, MySpace quickly became an

markets with strong direct network effects); *see also Microsoft Corp.*, 253 F.3d at 62 (finding Microsoft's misrepresentations in a market with direct network effects to be anticompetitive conduct under Section 2 of the Sherman Act).

[27] Market cap fluctuates with daily stock price changes. YAHOO FINANCE, https://finance.yahoo.com/quote/FB/ (last visited Jan. 21, 2019).

[28] For other discussions regarding competition based on quality rather than price, *see* Maurice E. Stucke & Ariel Ezrachi, *When Competition Fails to Optimize Quality: A Look at Search Engines,* 18 YALE J. OF L. & TECH. 70 (2016).

internet darling, especially in the wake of the dot-com bust of 2001. Within two years, in a heated bidding war between two media conglomerates, Rupert Murdoch's News Corp. and Sumner Redstone's Viacom, MySpace was acquired by News Corp. for $580 million dollars.[29] By 2006, MySpace overtook Google to become the most visited website in the U.S.[30] With a hundred million users, MySpace then signed a $900 million advertising deal with Google.[31] By 2007, dozens of competitors existed, but none matched the scale and growth of MySpace.[32] Journalists referred to the next generation, not as "millennials," but as the "MySpace generation."[33]

Though it looked as though MySpace had tipped the scales, and that it would inevitably become the de facto social media platform, it would not.[34] Mark Zuckerberg, the founder and chief executive officer of Facebook, and other enterprising entrepreneurs, had an opportunity for market entry to subvert MySpace's early gains. When Facebook rolled into the market, users,

---

[29] *See* Richard Siklos, *News Corp. to Acquire Owner of MySpace.com*, N.Y. TIMES (July 18, 2005), https://www.nytimes.com/2005/07/18/business/news-corp-to-acquire-owner-of-myspacecom.html.

[30] *See Hanging with the In-Crowd*, THE ECONOMIST (Sept. 14, 2006), https://www.economist.com/node/7918729.

[31] *Fox Interactive Media Enters into Landmark Agreement with Google Inc.*, NEWS FROM GOOGLE (Aug. 7, 2006), http://googlepress.blogspot.com/2006/08/fox-interactive-media-enters-into_07.html.

[32] Other social networking sites included SixDegrees.com, which launched 1997 and shut down 2001; Friendster, which launched 2002 and at one point, Friendster had over 115 million users and was the most used social network in Asia; Orkut, which was founded by Google in 2004 and shut down 2014; Flip.com, which was founded by Conde Nast in 2006 and shut down December 2008; Bebo, which was founded in 2005 and at one point was the most used social network in the U.K. and was purchased by AOL in 2008 for $850 million, but in 2010 AOL announced it would shut down or sell the site; Mixi, which was founded in 2004 and at one point was the largest social networking site in Japan; CyWorld, which was founded in 1999 and was once the primary social network in Korea, but declined after Facebook entered the market in 2009; hi5, which was launched 2004 and was a leading social network site in Spanish-speaking countries, including Mexico, Argentina, and Venezuela and is still in business; BlackPlanet , which was founded in 1999; a social network for African-Americans and is still in business; MiGente, which was founded 2001 for Latinos and is still operating; and Yahoo 360, which was Yahoo's effort at a social networking site with a soft-launch in 2005 that did not result in a full product launch.

[33] *See, e.g.,* Chris DeWolfe, *The MySpace Generation*, FORBES MAGAZINE (April 20, 2007), https://www.forbes.com/forbes/2007/0507/072.html#60433a9b569e; *The MySpace Generation*, BLOOMBERG.COM (Dec. 12, 2005), https://www.bloomberg.com/news/articles/2005-12-11/the-myspace-generation; Rhymer Rigbey, *Employers Target the MySpace Generation*, FINANCIAL TIMES (Aug. 7, 2006), https://www.ft.com/content/efce5b2a-2636-11db-afa1-0000779e2340.

[34] *See, e.g.*, John Barrett, *MySpace is a Natural Monopoly*, TECH NEWS WORLD (Jan. 17, 2007), https://www.technewsworld.com/story/55185.html; Victor Keegan, *Will MySpace ever Lose its Monopoly?*, THE GUARDIAN (New York), Feb. 8, 2007, https://www.theguardian.com/technology/2007/feb/08/business.comment.

parents, and critics were simultaneously gripped by an apprehension with social media, caused primarily by MySpace.[35] One could not ignore the barrage of negative MySpace headlines in the media, permeating radio stations, television broadcasts, and newspaper reporting, across the country.[36] MySpace was blamed for sexual assaults, suicides, and murders, allegedly triggered by open communications on the platform. Parents were concerned that MySpace was not safe for children,[37] and national and local news blamed the platform's openness and lack of privacy. Academia echoed this sentiment with consumer surveys demonstrating that social media users were concerned about privacy and that "MySpace, the largest social networking site in the world, has a poor reputation in terms of trust."[38]

Indeed, Facebook's disintermediation of MySpace's rise is the story of just how important Facebook's qualitative differentiation was. Since MySpace was already free, Facebook had to entice users with something unique. Thus, Facebook entered the market presenting itself, among other things, as a privacy-centered alternative. MySpace made little to no effort to address concerns around privacy, while Facebook appeared to take privacy seriously. Whereas MySpace

---

[35] *See* CHARLES KRINSKY, THE ASHGATE RESEARCH COMPANION TO MORAL PANICS (2016).

[36] *See, e.g.*, Sue Downes, *Teens Who Tell Too Much*, N.Y. TIMES (Jan. 15, 2006), http://www.nytimes.com/2006/01/15/opinion/nyregionopinions/teens-who-tell-too-much.html; Anna Bahney, *Don't Talk to Invisible Strangers*, N.Y. TIMES (May 9, 2006), https://www.nytimes.com/2006/03/09/fashion/thursdaystyles/dont-talk-to-invisible-strangers.html; Jane Gordon, *MySpace Draws a Questionable Crowd*, N.Y. TIMES (February 26, 2006), https://www.nytimes.com/2006/02/26/nyregion/nyregionspecial2/myspace-draws-a-questionable-crowd.html; John Kreiser, *MySpace: Your Kids' Danger*, CBS NEWS (Feb, 6, 2006), https://www.cbsnews.com/news/myspace-your-kids-danger/; *Myspace Murderer: An Epilogue*, WIRED (Nov. 17, 2006), https://www.wired.com/2006/11/myspace-murder-an-epilogue/; Tom Rawstorne, *How Pedophiles Prey on MySpace Children*, DAILYMAIL.COM (July 21, 2006), http://www.dailymail.co.uk/femail/article-397026/How-paedophiles-prey-MySpace-children.html; Noah Shachtman, *Murder on MySpace*, WIRED (Dec. 1, 2006), https://www.wired.com/2006/12/murderblog/; Brad Stone, *U.S. States Fault MySpace on Predator Issues*, N.Y. TIMES (May 15, 2007), https://www.nytimes.com/2007/05/15/technology/15iht-15myspace.5712603.html; Brad Stone, *New Scrutiny for Facebook Over Predators*, N.Y. TIMES (July 29, 2007), https://www.nytimes.com/2007/07/30/business/media/30facebook.html.

[37] *See, e.g.,* Julie Rawe, *How Safe is MySpace?* TIME MAGAZINE (June 26, 2006), http://content.time.com/time/magazine/article/0,9171,1207808,00.html; Susanna Schrobsdorff, *Predator's Playground*, NEWSWEEK (Jan. 26, 2006), http://www.newsweek.com/predators-playground-108471.

[38] Catherine Dwyer, Starr Hiltz & Katia Passerini, Americas Conference on Information Systems, *Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace* (2007).

was open to anyone who wanted to join, Facebook was closed to all but those who could validate their identity with a university-issued ".edu" email address. After joining, Facebook users encountered strict privacy settings—for example, the default setting was that only one's university classmates or one's friends could see one's profile.[39] On the other hand, on MySpace the default setting was more open—anyone could see one's profile. This is relevant because studies show that consumers do not change a website's default settings because it is cumbersome and time-consuming[40]—the modern-day equivalent of leaving the VCR clock blinking. A social network's default settings are therefore an important initial sales pitch.

Further signaling a commitment to privacy, Facebook almost immediately hired a chief privacy officer and articulated to users a short, plain-English, privacy policy that put privacy at the center of the user experience.[41] Only some 950 words long, the initial policy took only a few minutes to read. Indeed, just as the liberal return policy is designed to engender trust among prospective customers in e-commerce, so was Facebook's privacy policy designed to engender trust with early adopters of social media. The opening sentence proclaimed: "Because we want to demonstrate our commitment to our users' privacy, we will disclose our information and privacy

[39] Initially, Facebook users could not make their profile visible to everyone even if they wanted to. *See* Boyd & Ellison, *supra* note 4; DAVID KIRKPATRICK, THE FACEBOOK EFFECT: THE INSIDE STORY OF THE COMPANY THAT IS CONNECTING THE WORLD (2011); KATHERINE LOSSE, THE BOY KINGS: A JOURNEY INTO THE HEART OF THE SOCIAL NETWORK XV (2012).

[40] Wendy E. Mackay, *Triggers and Barriers to Customizing Software*, CONF. ON HUMAN FACTORS IN COMPUTING SYS.,153–160 (1991). S*ee also* Catherine Dwyer, *Digital Relationships in the" Myspace" Generation: Results From a Qualitative Study*, 40TH ANNUAL HAW. INT'L CONF. ON SYS. SCIS., 19 (2007) (after interviewing undergraduates that use social media and instant messenger applications, authors pointed out that most interviewees did not customize the privacy settings of their chosen platforms.); Ralph Gross & Alessandro Acquisti, Proceeding of the Ass'n for Computing Machinery Workshop, *Information Revelation and Privacy in Online Social Networks* 71–80 (2005) (authors studied the behavior of more than 4,000 students on Facebook and found that only 1.2% of users studied changed their privacy settings).

[41] Chris Kelly, who later ran for governor of California, was hired as Facebook's chief privacy officer in September of 2005.

practices ...."[42] Therein, Facebook made important representations regarding what it would and would not do. One important representation—whose evolution is the focus of this Paper —was the promise to not usurp privacy by using tracking technology.[43] Facebook promised: "We do not and will not use cookies to collect private information from any user."[44]

Without understanding tracking technology, it is impossible to understand how Facebook would eventually leverage its power to degrade user privacy and build a business model affecting data and advertising inventory across millions of independent businesses. The most common tracking methodology to surveil users leveraged the use of "cookies", small text files that websites can install on users' computers.[45] At a simple level, a cookie enables a website to identify a browser using a unique identifier, in order to remember a previous action on the part of the user. Cookies can be used to remember historical actions—such as if a user had put items into a shopping cart, if a user had already logged-in, or what a user normally enters in a form field. On an individual level, cookies can add to a user's welfare by allowing a website to improve the quality of the site's user experience.

---

[42] *Facebook Privacy Policy*, FACEBOOK.COM (Dec. 30, 2004), http://www.thefacebook.com/policy.php [https://web.archive.org/web/20050107221705/http://www.thefacebook.com/policy.php] [hereinafter "FACEBOOK PRIVACY POLICY (2004)"].

[43] *See id*. ("We use session ID cookies to confirm that users are logged in. These cookies terminate once the users close the browser. We do not and will not use cookies to collect private information from any user."); *see also Facebook Privacy Policy*, FACEBOOK.COM (effective February 27, 2006), http://www.facebook.com:80/policy.php [http://web.archive.org/web/20060222121022/http://www.facebook.com:80/policy.php] ("We use session ID cookies to confirm that users are logged in. These cookies terminate once the user closes the browser. By default, we use a persistent cookie that stores your login ID (but not your password) to make it easier for you to login when you come back to Facebook."); *Facebook Privacy Policy*, FACEBOOK.COM (effective Sept. 12, 2007), http://www.facebook.com/policy.php [http://web.archive.org/web/20070912083143/http://www.facebook.com/policy.php] [hereinafter FACEBOOK PRIVACY POLICY (2007)] ("When you enter Facebook, we collect your browser type and IP address. …… We use session ID cookies to confirm that users are logged in. These cookies terminate once the user closes the browser. By default, we use a persistent cookie that stores your login ID (but not your password) to make it easier for you to login when you come back to Facebook.").

[44] FACEBOOK PRIVACY POLICY (2004), *supra* note 42.

[45] *HTTP State Management Mechanism*, RFC-EDITOR.ORG (April 2011). https://www.rfc-editor.org/info/rfc6265.

Cookies, however, can also be used to determine what a user was researching, reading, or buying on a site. When a user types a website URL into a browser (such as nytimes.com), the user's computer initiates an HTTP request with the website's server. The website's server then sends back an HTTP response that allows the user to see the webpage. During HTTP responses, servers can also send back and implant cookies on a user's device. The cookies thumb-print a user's device with a unique identifier, or a "cookie ID" (for example, 123456789).[46] These cookies can then be "read" by the issuing company during a user's subsequent HTTP requests. When read, the user's cookies provide the user's cookie ID, and other elements of the HTTP request can provide specific information regarding the user's browser session, including: the specific URL the user is visiting (for example, goodmenproject.com/marriage-2/Coming-Out-To-Your-Wife/), the time the user is visiting said URL, and the IP address of the user (which discloses the user's geographic location). In this way, a company can use cookies to know (and therefore remember) the fact that user 123456789 was reading the article "Coming Out to Your Wife" on a Sunday morning at 5:30 a.m. from Wichita, KS.

Widespread commercial surveillance of consumer behavior across the internet, however, was inhibited by two restraining facts. First, a company could only read its own cookies. Second, a company could read cookies only when a user initiates an HTTP request to the company's server. For example, if The New York Times wrote a cookie onto a user's device, the Times could not read its cookies when the user was on wsj.com. In other words, The Times could know what users were doing on nytimes.com but not on other properties. A company could circumvent these built-in privacy protections by installing a piece of their own code on other websites, that would invisibly generate an HTTP request on behalf of the user to the company's server. Of

[46] Cookies were initially invented with randomized ID numbers instead of permanent ones attributed to a user's browser precisely to avoid "cookies [being] used as a general tracking mechanism." *See* John Schwartz, *Giving Web a Memory Cost Its Users Privacy,* N.Y. TIMES (Sept. 4, 2001), https://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html.

course, no publisher would want another publisher to be tracking the behavior of its own customers. In order to develop complete and accurate profiles of users, there would need to be cooperation among thousands of sites which would otherwise be competitive. At one point, competitors and competition kept horizontal cookie collusion in check.

When Facebook first entered the market, and for the next ten years, Facebook promised to not surveil users for commercial purposes. This promise was not de minimis. As an electronic communications service provider, Facebook knew people's real identities and therefore could correlate anonymous cookie IDs with real world identities. You weren't just 123456789 reading the article titled "Coming Out to Your Wife," you were Jacob Greenberg of Wichita, KS reading "Coming Out to Your Wife." Additionally, numerous studies showed that consumers were concerned about privacy and objected to behavioral (or psychographic) targeted digital advertising.[47] Aside from broader objections to surveillance, which is known to quell research and speech, surveillance had immediate practical implications within the household. If a company could know that Ms. Mitchell was shopping for that Star Wars Lego set that was all the rage that season, it could incessantly display on the family computer ads for the same toy, which could potentially ruin for young Sam what Santa Claus was bringing for Christmas.

Although this Paper focuses on the evolution of the promise not to surveil users outside of Facebook, for which there is a rich historical record of Facebook's conduct both pre and post market dominance, it is worth noting that Facebook made other significant privacy

[47] Online privacy and the ability to browse, read, shop, and think online without being watched has been a consumer concern since the turn of this century. *See* Chris Jay Hoofnagle, Jennifer Urban & Su Li, *Privacy and Advertising Mail*, BERKELEY CENT. FOR L. AND TECH. (2012), http://ssrn.com/abstract=2183417; M. J. Metzger & S/ Docter, *Public Opinion and Policy Initiatives For Online Privacy Protection*. 47 J. OF BROADCASTING & ELEC. MEDIA 3 (2003); Schwartz, *supra* note 46 (2001 survey by Public Opinion Strategies, a Republican polling organization, showed 67% of Americans said "online privacy" was a "big concern"); *U.S. Internet Users Ready to Limit Online Tracking for Ads*, News.Gallup.Com (Dec. 21, 2010), https://news.gallup.com/poll/145337/internet-users-ready-limit-online-tracking-ads.aspx (2010 USA Today/Gallup poll showed Americans were aware of cookies and behavioral advertising, 67% said marketers should not be able to conduct behaviorally targeted advertising, and 61% said free internet services do not justify the practice).

representations upon entering the market.[48] For example, Facebook initially gave users the ability to opt-out of having their information shared with third-parties, including advertisers or marketers, or to prohibit Facebook from collecting additional information about themselves from third-parties.[49] Facebook also initially promised that users could modify or remove information Facebook had about them at any time. These promises combined signaled to users that, unlike other social networks, Facebook offered its members "very granular and powerful control on the privacy … of their personal information."[50] The combination of Facebook's closed network approach and strict default privacy settings made people believe that Facebook, and not MySpace, was the trustworthy choice.

Facebook's short privacy policy, default privacy settings, and outward signaling as privacy-centric, were strategic decisions that played an important role in attracting users to the platform. David Kirkpatrick, who chronicles Facebook's history in his book *The Facebook Effect*, summarizes, "Privacy … has been a major concern of Facebook's users from the beginning."[51] For example, for Katherine Losse, one of Facebook's first employees, Facebook's unique stance on privacy was a critical part of her decision to join a social media platform. She explained, "The privacy protections of the restricted network … made it feel, surprisingly, okay."[52] Accordingly, early consumer studies revealed that the broader population possessed similar feelings for privacy concerns.[53] The majority of Americans polled in one 2004 national

---

[48] For a general overview of Facebook's progressive deterioration of user privacy, see Jennifer Shore & Jill Steinman, *Did You Really Agree to That? The Evolution of Facebook's Privacy Policy*, TECH. SCI. (2015), https://techscience.org/a/2015081102.

[49] FACEBOOK PRIVACY POLICY (2004), *supra* note 42.

[50] Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, INT'L WORKSHOP ON PRIVACY ENHANCING TECHS. 2 (2006) [hereinafter "*Imagined Communities*"].

[51] *See* Kirkpatrick, *supra* note 39 at 13.

[52] *See* Losse, *supra* note 39 at XV.

[53] David Stark & C. Hodge, *Consumer Behaviors and Attitudes About Privacy: A Tns/Truste Study*, TNS/TRUST 13 (2004), http://www.truste.org/pdf/Q4_2004_Consumer_Privacy_Study.pdf.

consumer study said privacy was a "really important issue that [they] care about often."[54] Another survey focused on early Facebook users' attitudes towards privacy and concluded that Facebook users cared about privacy policy more than terrorism.[55] Others in academia studied and compared MySpace users' satisfaction with MySpace's privacy settings with Facebook users' satisfaction with Facebook's privacy settings and concluded that users generally preferred Facebook's settings over MySpace's settings.[56]

Indeed, increased levels of privacy are broadly understood to be the mechanism that induces people to trust and then communicate over a particular communications channel. For example, social exchange theory, with a foot simultaneously in economics, psychology and sociology, studies human communications and explains that people communicate and form relationships through a simple cost-benefit analysis[57]: the benefit is the opportunity to socialize, and the cost is the risk associated with trusting someone. Privacy increases trust and reduces risk, thereby causing humans to communicate more. In the real word, the lack of a permanent record ensures some level of privacy.[58] Online, a social network that wants users to choose its platform over others could generate superior trust through superior promises of privacy.

Privacy continues to play an important role in the current, though less competitive, social media market. SnapChat is the only social network post-2010 to have gained significant adoption with users in the United States.[59] Like Facebook once did, SnapChat competes on quality, and

---

[54] *Id*.

[55] *See* Acquisti & Gross, *Imagined Communities*, *supra* note 50 at 6.

[56] *See* Acquisti & Gross, *Imagined Communities*, *supra* note 50 at 16; Dwyer, Hiltz & Passerini, *supra* note 38 at 339.

[57] *See* Donna L. Hoffman, Thomas P. Novak & Marcos Peralta, *Building Consumer Trust Online*, 42 COMMS. OF THE ACM 80–85 (1999); *see also* Miriam J. Metzger, *Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce*, 9 J. OF COMPUTER-MEDIATED COMM. 942 (2004); MICHAEL E. ROLOFF, INTERPERSONAL COMMUNICATION: THE SOCIAL EXCHANGE APPROACH (1981).

[58] Consider Lawrence Lessig's prescient essay on internet threats to privacy: Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. ENT. L. AND PRACTICE 56-65 (1999).

[59] *See* STATISTA.COM, *infra* note 237.

importantly, on privacy levels. For example, one of the central draws of SnapChat is the fact that SnapChat communications appear for a fixed period of time, then disappear, being also deleted from SnapChat's servers.[60] The impermanency of the record ensures a high degree of privacy. Additionally, when Facebook users discovered in early 2017 that Facebook was collecting and sharing user data in ways previously not known or understood, users instigated a #deleteFacebook movement, and millions flocked to startup competitor Vero Social that promised significantly higher levels of privacy.[61]

The fact that communications markets turn on privacy is history repeating itself. Wireless telegraphy, before eventually being used to facilitate what we know today as the modern radio, initially stalled as a technology because of its inability to facilitate private communications.[62] Moreover, this nation's historic antitrust case against and eventual break-up of AT&T in the telephone network market was instigated in part by an equipment competitor's desire to offer telephone equipment that offered a higher level of privacy in communications.[63] Until 1956, customers of AT&T's telephone service were required to use AT&T telephone equipment to make and receive calls. Equipment manufacturer Hush-A-Phone marketed a cup-like device that attached to AT&T equipment to reduce the risk of conversations being overheard. Consumers purchased over 125,000 Hush-A-Phones to make for "privacy in communications" and in 1948, Hush-A-Phone filed a complaint with the Federal Communications Commission requesting that

---

[60] *When Does Snapchat delete Snaps and Chats?*, SNAPCHAT.COM, https://support.snapchat.com/en-US/a/when-are-snaps-chats-deleted, (last visited Jan. 21, 2019).

[61] *See* Ben Gilbert, *#DeleteFacebook Is Trending: Here's How to Delete Your Facebook Account*, BUSINESSINSIDER.COM (March 18, 2018), https://www.businessinsider.com/how-to-delete-facebook-2018-3; *see also* Ann-Marie Alcantara, *Could This Social Media Ad-Free App Go Mainstream Amid Facebook's Privacy Woes?,* ADWEEK.COM (April 12, 2018), https://www.adweek.com/digital/this-ad-free-social-media-app-thinks-it-can-capitalize-on-facebooks-privacy-woes/.

[62] BHU SRINIVASAN, AMERICANA:THE 400-YEAR HISTORY OF AMERICAN CAPITALISM 293 (2017).

[63] JEAN-JACQUES LAFFONT & JEAN TIROLE, COMPETITION IN TELECOMMUNICATIONS 18 (1999).

the FCC compel AT&T to officially permit customers' use of Hush-A-Phone equipment. [64] Hush-A-Phone eventually prevailed and this opened the door to competition in the market for telephone equipment.[65]

In the early 2000s, Facebook entered the social media market, disintermediated MySpace's momentum, and started to consolidate the social network market by offering consumers an alternative service of superior quality. Other qualitative features, like Facebook's user interface design, real-name policy, and college launch strategy, also played a role in making Facebook's platform attractive to users.[66] Regardless, the fact remains that superior privacy levels played a central role in this narrative. Propelled then by direct network effects, whereby each additional user that chose Facebook made the Facebook network more attractive to the next incremental user, Facebook started to consolidate the social network market at a rapid rate, taking market share from MySpace, Friendster, and competitive offerings from Google and AOL. At the end of 2004, MySpace had 5 million users and Facebook had 1 million users.[67] In 2006, when some 250 million people around the world used a social network, 100 million used MySpace, 12 million used Facebook, and the rest were dispersed across numerous competitors.[68] Then, in 2007, user growth at MySpace started to decelerate, while growth at Facebook accelerated. By mid 2007, Facebook had overtaken MySpace as the most visited social media

---

[64] For the court of appeals decision, *see* Hush-A-Phone v. United States, 238 F.2d 266 (D.C. Cir. 1956).

[65] *Id*.

[66] For example, Sean Parker, Facebook's first president, has explained that Facebook's strategy in first dominating the social media market, and general product development, were important reasons that users chose Facebook over MySpace. Alexia Tsotsis, *Sean Parker on Why MySpace Lost to Facebook*, TECHCRUNCH.COM (June 28, 2011), https://techcrunch.com/2011/06/28/sean-parker-on-why-myspace-lost-to-facebook/. Others have partly attributed Facebook's superior product to superior design. *See, for e.g.*, Jenna McWilliams, *How Facebook Beats MySpace*, THE GUARDIAN (June 23, 2009), https://www.theguardian.com/commentisfree/cifamerica/2009/jun/23/facebook-myspace-social-networks.

[67] *Number of Active Users at Facebook Over the Years*, YAHOO! FINANCE (Oct. 23, 2012), https://finance.yahoo.com/news/number-active-users-facebook-over-years-214600186--finance.html.

[68] *Id*.

network in the U.S.[69] One year later, MySpace stopped growing, while Facebook was registering half-a-million new users per day.[70] Today, of course, MySpace, Orkut, Bebo, and other competitors, are relics of the early history of social media. Facebook dominates the life of the average American—99% of adults that use any form of social media use Facebook, and the average American now spends over an hour per day on Facebook applications.[71]

II. THE PARADOX OF SURVEILLANCE REFLECTS MONOPOLY POWER

Monopoly power refers specifically to the power to control a market—that is, the power in a market to raise price above or reduce quality below competitive levels.[72] From a legal standpoint, the question of whether a company has monopoly power in a market is answered through direct or indirect evidence. Indirect evidence focuses on a company's percent share of a relevant market, amongst other structural factors that indicate a company's hold on a market (e.g., entry barriers).[73] Direct evidence, on the other hand, demonstrates a company's acquired ability to increase price above or decrease quality below levels unsustainable in a previous competitive environment.[74] Under the direct evidence approach, the strongest type of evidence is evidence of price or quality levels pre-power, an event or point in time which results in power,

---

[69] Erick Schonfeld, *Facebook Blows Past MySpace in Global Visitors for May*, TECHCRUNCH.COM (June 20, 2008), https://techcrunch.com/2008/06/20/facebook-blows-past-myspace-in-global-visitors-for-may/.

[70] *Id.*

[71] *See* Social Media Fact Sheet, PEW RES. CTR. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/social-media/ (69% of U.S. adults use social media; 68% of U.S. adults use Facebook). *Average Time Spent per Day with Facebook, Instagram, and Snapchat*, EMARKETER.COM (June 1, 2018), https://www.emarketer.com/Chart/Average-Time-Spent-per-Day-with-Facebook-Instagram-Snapchat-by-US-Adult-Users-of-Each-Platform-2015-2020-minutes/219352.

[72] *See generally* United States v. E. I. du Pont de Nemours & Co., 351 U.S. 379, at 391 (1956) [hereinafter "du Pont"].

[73] United States v. Microsoft Corp., 253 F.3d 34, 51 (D.C. Cir. 2001) ("...monopoly power may be inferred from a firm's possession of a dominant share of a relevant market that is protected by entry barriers."); United States v. Grinnell Corp., 384 U. S. 563, 571 (1966).

[74] *See du Pont*, 351 U.S. at 391 (explaining that "monopoly power is the power to control prices"); Standard Oil Co. of New Jersey v. United States, 221 U.S. 1 (1911).

and evidence of price increases or quality degradations that would have previously been unsustainable.[75] This fact-based, retrospective before-and-after analysis—though somewhat rare in antitrust cases—is particularly relevant in Facebook's case.

Part II now tells the story of how it came to be that Facebook extracts from consumers an exchange founded on surveillance. Contrary to what many believe, digital surveillance is not simply the inevitable byproduct of how the internet works. Rather, promises of privacy were the deciding factors that tipped the early market in Facebook's favor, away from MySpace. Facebook's conduct, from 2004-2012, provides the benchmark of quality—at least with respect to commercial surveillance—that the restraining forces of competition demanded. By 2014, competitors had exited the market, Google's competitive offering Orkut shut down,[76] and Facebook's monopoly was complete due to the exit of competition combined with the protection of the barrier to entry that results from a product with over a billion users on a closed communications network. Subsequently, in 2014, Facebook leveraged its market power in a consolidated market to successfully degrade privacy to levels unsustainable in the earlier competitive market when market participants were subject to consumer privacy demands. Facebook rapidly unraveled its promise not to conduct commercial surveillance by using the technical framework it built over the years by perpetuating the belief that it would not leverage such a framework for a commercial purpose.

A. PRE-POWER: Failure of Beacon and Early Misrepresentations

[75] *See generally* Daniel A. Crane, *Market Power Without Market Definition*, 90 NOTRE DAME L. REV. 31 (2014).

[76] *See* Ellen Huet, *Google Finally Shuts Down Orkut, Its First Social Network*, FORBES MAGAZINE (June 30, 2014), https://www.forbes.com/sites/ellenhuet/2014/06/30/google-kills-orkut/#2874fded634b.

By 2007, people were sharing more baby pictures and personal family and friend photos on Facebook than they were on any other social media site—MySpace was edgy, Facebook was wholesome.[77] Then on November 6, 2007, with growing momentum in the market, Facebook reneged on the promise not to surveil users outside of Facebook through the release of an advertising product called "Beacon."[78] Beacon was a direct product license to third-parties that openly allowed Facebook to monitor and record user activity off of Facebook, and reflects Facebook's first attempt to track users on the sites of independent businesses.[79] But Beacon was immediately controversial. Its ultimate failure is evidence of what competition demanded of Facebook from a privacy perspective.

Launched in conjunction with a handful of third-parties, including Blockbuster and The New York Times, Facebook provided Beacon participants a piece of Facebook code to install on their own sites.[80] When a user triggered an action on a participating site (say, rented a movie or read an article), the website then presented the user with a pop-up box requesting permission to share the user's activity on Facebook.[81] Many people today would remember being once jarred by the pop-up requesting permission to share one's reading or browsing activity with Facebook. The user could decline permission by selecting the "No, Thanks" option.[82] If the user did *not*

---

[77] *Facebook's Mark Zuckerberg: Hacker. Dropout. CEO.*, FASTCOMPANY.COM (May 1, 2007), https://www.fastcompany.com/59441/facebooks-mark-zuckerberg-hacker-dropout-ceo.

[78] *Leading Websites Offer Facebook Beacon for Social Distribution*, NEWSROOM.FB.COM (NOV. 6, 2007), https://newsroom.fb.com/news/2007/11/leading-websites-offer-facebook-beacon-for-social-distribution/; *see also Facebook Announces Facebook Ads, Beacon in New York*, ADWEEK.COM (Nov. 6, 2007), https://www.adweek.com/digital/facebook-announces-facebook-ads-beacon-in-new-york/.

[79] NEWSROOM.FB.COM, *supra* note 78.

[80] *Id.*

[81] Michael Arrington, *Ok Here's At Least Part of What Facebook is Announcing on Tuesday: Project Beacon*, TECHCRUNCH.COM (Nov. 2, 2007), https://techcrunch.com/2007/11/02/ok-heres-at-least-part-of-what-facebook-is-announcing-on-tuesday/.

[82] Users could have opted-in (via Facebook settings) to always include activity on third-party sites on their News Feed, opted-out to never include it, or opted-in to include it only if the user did not opt-out when given the pop-up confirmation (default). For a short history of Beacon's changing user-interface against a backdrop of consumer uproar, see Louise Story, *The Evolution of Facebook's Beacon*, N.Y. TIMES (Nov. 29, 2007), https://bits.blogs.nytimes.com/2007/11/29/the-evolution-of-facebooks-beacon/.

click the "No, Thanks" button, Facebook received information about the user's activity (title of movie rented or article read).[83] Then, Facebook would publish the activity on the user's Facebook page, calling the publication a "social advertisement."[84] For Beacon participants, like The New York Times or Conde Nast, the social sharing of user activity was a type of free marketing.

Screenshot of the Beacon pop-up displayed to users on third-party sites.[85]

Beacon was a transparent attempt to get users to consent to sharing information about their activity on third-party sites with Facebook. However, the mere presence of Facebook's code on these sites made it technically possible for Facebook to track users' activities on these sites, even if the user did not grant Facebook permission to do so. This is because, when a user visited a Beacon site (e.g., blockbuster.com), regardless of whether the user consented or not, Facebook code initiated an HTTP request on behalf of the user to Facebook's servers. Through this newly opened connection, Facebook could write cookies on user computers during HTTP responses, or read cookies during HTTP requests. The requests and cookies could reveal the specific page a user was on—effectively allowing Facebook to accomplish surveillance on the users that had clicked "No, Thanks."

[83] According to Facebook at the time, Facebook tracked and recorded the activity only of logged-in users who did not click the "No, Thanks" button.

[84] *See* Arrington, *supra* note 81.

[85] *Id*.

At the time, Facebook claimed that Beacon only tracked and monitored the activities of consenting users, and that Facebook code was not used to conduct less overt surveillance through cookies. For example, in a follow-up to emerging, strong, user push-back on the new Beacon product,[86] The New York Times interviewed Facebook's vice president of marketing and operations, Chamath Palihapitiya.[87] The reporter asked, "If I buy tickets on Fandango, and decline to publish the purchase to my friends on Facebook, does Facebook still receive the information about my purchase?" Palihapitiya answered, "Absolutely not. One of the things we are still trying to do is dispel a lot of misinformation that is being propagated unnecessarily."[88] Facebook represented that it did not receive information about users that declined to share information about their activity.

Only hours after Palihaptiya's comments in the Times, Stefan Berteau, a senior research engineer at California's Threat Research Group, examined the actual contents of Facebook's HTTP requests and responses that were normally invisible to users, and revealed that Palihapitiya's representations were not true.[89] While Facebook claimed that Beacon trackers did not transmit user information to Facebook if users clicked "No, Thanks", the contents of the cookie files did just that.[90] Berteau further revealed that Beacon trackers were also used to log

---

[86] *See* Nick O'Neill, *MoveOn.org to Challenge Facebook Beacon,* ADWEEK.COM (Nov. 20, 2007), www.adweek.com/digital/moveonorg-to-challenge-facebook-beacon/.

[87] Brad Stone, *Facebook Executive Discusses Beacon Brouhaha,* N.Y. TIMES (Nov. 29, 2007), https://bits.blogs.nytimes.com/2007/11/29/facebook-responds-to-beacon-brouhaha/.

[88] *Id*.

[89] Stefan Berteau, *Facebook's Misrepresentation of Beacon's Threat to Privacy: Tracking Users Who Opt Out or Are Not Logged In*, CA SECURITY ADVISOR RES. BLOG, (Dec. 1, 2007), https://www.techmeme.com/071201/p3#a071201p3.

[90] *Id. (*Berteau showed, for example, that if a user saved a recipe on Epicurious to a favorites folder, and explicitly declined to have this information publish to his Facebook profile, the Beacon program wouldn't publish it, but would nonetheless share the information about what the user was doing on the Epicurious website with Facebook). S*ee also* Juan Carlos Perez, *Facebook's Beacon More Intrusive than Previously Thought*, PCWORLD.COM (Nov. 30, 2007), https://www.pcworld.com/article/140182/article.html.

the activity of users who logged-out of Facebook or did not have a Facebook account.[91] Furthermore, if a logged-out user ever clicked the "Remember Me" checkbox when logging-in, Facebook actively associated cookies with a user's Facebook ID number.[92] In other words, Facebook linked normally anonymized cookie data back to the identities of real people—a connection Facebook could make because it operated the social network.

Indeed, Facebook's Privacy Policy at the time did not obtain user consent for this practice. As displayed on November 29, 2007, Facebook claimed that it only used cookies to "confirm that users are logged in" and that "[t]hese cookies terminate once the user closes the browser."[93] Within a few days, Facebook confirmed Berteau's findings, contradicting its own earlier representations about user privacy.[94] For the first time, Facebook had been publicly caught using cookies for broader surveillance despite the promise it did not and would not do so.

Almost immediately, Facebook faced user protest, petitions from advocate groups, and class action lawsuits. A MoveOn.org petition garnered 50,000 signatures within days.[95] Class-action lawsuits on behalf of users were filed in Texas and California.[96] The page of another petition called "Facebook, stop invading my privacy," stated: "A lot of us love Facebook - it's helping to revolutionize the way we connect with each other. But they need to take privacy

---

[91] *See* Berteau, *supra* note 89; s*ee also* Juan Carlos Perez, *Beacon's User Tracking Extends Beyond Facebook, CA Says*, COMPUTERWORLD.COM (Dec. 3, 2007), https://www.computerworld.com/article/2537951/data-privacy/beacon-s-user-tracking-extends-beyond-facebook--ca-says.html.

[92] *See* Berteau, *supra* note 89; Perez, *supra* note 90.

[93] FACEBOOK PRIVACY POLICY (2007), *supra* note 43.

[94] *See* Perez, *supra* note 90.

[95] *See* O'Neill, *supra* note 86;
Ellen Nakashima, *Feeling Betrayed, Facebook Users Force Site to Honor Their Privacy*, WASH. POST (Nov. 30, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/11/29/AR2007112902503.html?noredirect=on.

[96] *See* Harris v. Blockbuster Inc., 622 F. Supp. 2d 396 (N.D. Tex. 2009); Lane v. Facebook Inc., 696 F.3d 811 (9th Cir. 2012).

seriously."[97] Facebook was founded upon the qualitative promise of no surveillance outside of Facebook and users did not want this to change. Consumer resistance is early proof of consumers' preference for no surveillance.

Rejection of Facebook surveillance on third-party sites was part of a wider rejection of all third-party cookie tracking as consumers tried to stop this type of commercial surveillance that the advertising industry coordinated to impose on consumers.[98] A 2005 industry study showed that 67% of Americans wanted to protect their privacy and prevent tracking.[99] Some advertising companies paid businesses for the ability to install their own code on the business' websites to track the business' customers.[100] One such company was Seevast. Seevast's code triggered an open connection between a business' website visitors and Seevast's servers, which Seevast used to install cookies on, and retrieve cookies from, the business' users.

Unlike companies like Seevast, Facebook knew users' real identities, and nearly fifty million people had a Facebook account.[101] Facebook's surveillance, unlike Seevast's, could be tied not only to random cookie variables, but to peoples' real names. In other words, Facebook could leverage the ability to identify people through use of the century's new communications technology, to conduct a particularly invasive, and permanent, form of surveillance.

---

[97] *See* Eric Auchard, *Facebook Alters Notifications after Privacy Furor*, REUTERS.COM (Nov. 29, 2007), https://www.reuters.com/article/us-facebook-privacy-idUSN2925736120071130.

[98] For example, consumers' cookie deletion rates rose at a rapid clip starting in 2004 when the advertising industry started to use cookies for tracking. Subsequently, the digital ad industry association group Interactive Advertising Bureau (IAB) and Safecount announced an initiative to cut cookie deletion rates. *See* Mickey Khan, *Rising Cookie Rejection Bites into Metrics*, DMNEWS.COM (July 11, 2005), https://www.dmnews.com/customer-experience/news/13074659/rising-cookie-rejection-bites-into-metrics. *See also* Chris Jay Hoofnagle, Jennifer King, Su Li & Joseph Turow, *How Different are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies?* (2010), https://repository.upenn.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1413&context=asc_papers (finding that 39% of American Internet users delete all their cookies "often").

[99] *See* Khan, *supra* note 97 (citing study from online market researcher InsightExpress).

[100] *See* Saul Hansell, *Facebook Retreats on Online Tracking,* N.Y. TIMES (Aug. 15, 2006), https://www.nytimes.com/2006/08/15/technology/15search.html.

[101] S*ee* Julie Sloane, *Facebook Got Its $15 Billion Valuation — Now What?* WIRED (Oct. 26, 2007), https://www.wired.com/2007/10/facebook-future/.

Additionally, Facebook did not have to pay companies, it could simply leverage the power to give away something valuable for free.

In the face of backlash, some Beacon participants pulled out of the Beacon program, effectively declining to extract consent from their own website visitors to Facebook's surveillance mechanism. The growing e-retailer Overstock, one of the initial companies to sign up for Beacon, pulled out. Their senior vice president of corporate affairs said, "we need to make sure that the Facebook community is accepting of this new type of advertising."[102]

In a competitive market, Facebook likely worried that strong user discontent around privacy would disrupt its momentum. While MySpace faced stagnating user growth, it still had double Facebook's number of users.[103] Google's Orkut had lost steam, but Google and MySpace recently announced they would join forces on Google's new OpenSocial initiative.[104] Orkut, Friendster, and Netscape co-founder Marc Andreessen announced support for OpenSocial.[105] In the U.K., a key battleground for the social media market, MySpace and Bebo still had the most users.[106] Additionally, competitors displayed an appreciation of having to compete with Facebook on matters related to user privacy. One such savvy competitor was MySpace's parent company, News Corp. An analyst with Jupiter Research remarked to CNN Money, "News Corp.

---

[102] Caroline McCarthy, *Facebook's Zuckerberg: 'We Simply Did a Bad Job' Handling Beacon*, CNET.COM (Dec. 5, 2007), https://www.cnet.com/news/facebooks-zuckerberg-we-simply-did-a-bad-job-handling-beacon/. *See also* Louise Story, *Coke Is Holding Off on Sipping Facebook's Beacon*, N.Y. TIMES (Nov. 30, 2007), https://bits.blogs.nytimes.com/2007/11/30/coke-is-holding-off-on-sipping-facebooks-beacon/?mtrref=undefined&gwh=59CBD7EC0914ECD5FCAB88B8BBF2201A&gwt=pay.

[103] *See* Sloane, *supra* note 101.

[104] *See* Jacqui Cheng, *Google Goes After Facebook With New OpenSocial Social Networking API,* ARSTECHNICA.COM (Nov. 1, 2007), https://arstechnica.com/uncategorized/2007/11/google-goes-after-facebook-with-new-opensocial-social-networking-api/.

[105] *See* Marc Andreessen, *Open Social: A New Universe of Social Applications All Over the Web*, BLOG.PMARCA.COM (Oct. 31, 2007), http://blog.pmarca.com/2007/10/open-social-a-n.html, [http://web.archive.org/web/20071102041108/http://blog.pmarca.com/2007/10/open-social-a-n.html] (Andreesen wrote on his blog, "We will aggressively support Open Social in every conceivable way.").

[106] *See* Rory Cellan-Jones, *Facebook Dismisses Privacy Fears*, BBC NEWS (Sept. 12, 2007), http://news.bbc.co.uk/2/hi/technology/6990767.stm (citing Nielsen netRatings and comScore numbers).

and Fox recognize the importance of allowing people to be alone with their friends, so they do not feel like they are being looked at by Big Brother. They understand how many competitors they have nipping at their heels right now, so they are doing everything they can not to alienate users."[107]

With numerous competitors nipping at Facebook's heels, Facebook retreated almost immediately after launching Beacon. Zuckerberg apologized and announced that Facebook would allow users to opt-out of the Beacon program.[108] But consumers did not accept Facebook's opt-out scheme, which required them to navigate Facebook's default privacy settings. Consumer uproar persisted, and, by September of the following year, Facebook revealed it would shut down Beacon entirely. Zuckerberg would later call Beacon a "mistake."[109]

Facebook's retreat with Beacon is evidence of what competition demanded of Facebook at the time. Following subsequent calls for regulation, Randall Rothenberg, the President and CEO of the Internet Advertising Bureau, the industry's trade association, wrote an op-ed in *The Wall Street Journal*, proclaiming that users' ability to resist Facebook's privacy changes was testament to the free market's ability to regulate itself.[110] Rothenberg, of course, was wrong.

---

[107] Paul R. La Monica, *Move Over, MySpace Social Networking is Hot - and There's More to the Rapidly Growing Market than MySpace and Facebook*, CNN.COM (Mar. 20, 2007), http://money.cnn.com/2007/03/19/news/companies/socialnetworks/index.htm.

[108] *See* Erick Schonfeld, *Zuckerberg Saves Face, Apologizes For Beacon,* TECHCRUNCH.COM (Dec. 5, 2007), https://techcrunch.com/2007/12/05/zuckerberg-saves-face-apologies-for-beacon/; Vauhini Vara, *Facebook Rethinks Tracking Site Apologizes, Makes it Easier to Retain Privacy*, WALL STREET J. (Dec. 6, 2007), https://www.wsj.com/articles/SB119687856122414681?mod=searchresults&page=3&po=18s;

[109] *See* Mark Zuckerberg, *Thoughts on Beacon*, BLOG.FACEBOOK.COM (Dec. 5, 2007), http://blog.facebook.com/blog.php?post=7584397130, [https://web.archive.org/web/20080107025500/http://blog.facebook.com/blog.php?post=7584397130]; and Mark Zuckerberg, *Our Commitment to the Facebook Community,* NEWSROOM.FB.COM (Nov. 29, 2011), https://newsroom.fb.com/news/2011/11/our-commitment-to-the-facebook-community/. For a history of Zuckerberg's apologies, *see* Geoffrey A. Fowler & Chiqui Esteban, *14 Years of Mark Zuckerberg Saying Sorry, Not Sorry*, WASH. POST (April 9, 2018), https://www.washingtonpost.com/graphics/2018/business/facebook-zuckerberg-apologies/?utm_term=.dbcff8504c9.

[110] Randall Rothenberg, *Facebook's Flop*, WALL STREET J. (Dec. 14, 2007), https://www.wsj.com/articles/SB119760316554728877?mod=searchresults&page=3&pos=16 (writing "Internet consumers have shown themselves willing and able to police the medium on their own. Just ask Facebook:

On the heels the Beacon controversy, and competitors' rising awareness of the importance of privacy to consumers, Facebook took the unprecedented step of announcing that future privacy changes would be subject to user approval. [111] Under a newly announced democratic process, incorporated into Facebook's governing documents, Facebook bound itself to allowing users to vote on future changes to important documents that contractually change user privacy—including the Privacy Policy, and other policies such as the Statement of Rights and Responsibilities and The Facebook Principles. Facebook's press release announced that the voting procedure "offers its users around the world an unprecedented role in determining the future policies governing the service."[112] In a rarely given public press conference, Zuckerberg explained that Facebook was doing this because social media users "feel a visceral connection to their rights. ... We are one of the only services on the web where people are sharing pretty personal and intimate information ... We're making it so that we can't just put in a new terms of service without everyone's permission. We think these changes will increase the bonding and trust users place in the service." [113]

The promise to let users vote on future privacy changes assured users that Facebook would not leverage its growing power to undermine users' privacy without users' meaningful consent. Facebook was already earning healthy profits on its exchange with users. In 2009,

---

Consumer regulation proved itself to be a far more effective, efficient, economically productive and unforgiving mechanism than federal regulation ever will be.").

[111] *See Facebook Announces First-Ever User Vote on Terms of Service Changes*, ADWEEK.COM (Apr. 6, 2009), https://www.adweek.com/digital/facebook-announces-first-ever-user-vote-on-terms-of-service-changes/; *Facebook Drafts New Governing Documents, Adopts New User Voting Process on Policy Changes*, ADWEEK.COM (Feb. 26, 2009), https://www.adweek.com/digital/facebook-drafts-new-governing-documents-process-for-user-voting-on-policy-changes/.

[112] *Facebook Opens Governance of Service and Policy Process to Users*, NEWSROOM.FB.COM (Feb. 26, 2009), https://newsroom.fb.com/news/2009/02/facebook-opens-governance-of-service-and-policy-process-to-users/

[113] Facebook's general counsel Ted Ullyot, and Facebook's vice president of privacy were also present. *See* Rafe Needleman, *Live Blog: Facebook Press Conference on Privacy*, CNET.COM (Feb. 26, 2009), https://www.cnet.com/news/live-blog-facebook-press-conference-on-privacy/.

Facebook earned $229 million in profits on $777 million in revenues.[114] In 2010, it earned $606 million on $1.974 billion.[115] Profit margins were 29% and 30% respectively—not quite as high as today's 47% but healthy nonetheless. But as Facebook's market power grew through the foreclosure of competition and the lock-in of network effects, Facebook would eventually abolish this newly announced voting procedure and reinstate the scope, scale, and invasiveness of Beacon's mission. Today, Facebook surveillance is a mandatory tie-in with a third-party's (e.g., The New York Times) use and license of other Facebook business products (Like buttons, Logins, etc.).

B. PRE-POWER: More Backtracking and Pattern of Conduct

This section traces the subsequent development of Facebook's "social plugin" products on the heels of Beacon's retreat. This early history of Facebook plugins is relevant to an antitrust inquiry for three reasons. First, history reveals that competition continued to restrain Facebook's ability to initiate surveillance. Second, Facebook's surveillance framework today requires the coordination of millions of independent third-parties. Facebook induced publishers and others to first coordinate with Facebook upon the representation that Facebook would not leverage their coordination for commercial surveillance. Third, the record opens the door to consider in Part IV whether Facebook's pattern of conduct reflects an anticompetitive acquisition of monopoly power under Section 2 of the Sherman Act.

---

[114] *See* FACEBOOK INC., REGISTRATION STATEMENT (Form S-1) (Feb. 1, 2012), https://www.sec.gov/Archives/edgar/data/1326801/000119312512034517/d287954ds1.htm [hereinafter "FACEBOOK S-1"].

[115] *Id.*

The relevant history of Facebook social plugins centers around the "Like" button—introduced early in 2010, at Facebook's annual F8 developer conference.[116] The Facebook Like buttons, and even the Login buttons,[117] are products offered to publishers and other independent businesses to improve site functionality and increase revenue. For publishers, the Like buttons, offered a turn-key review and distribution mechanism.[118] Facebook explained, "[e]ach Like creates distribution on Facebook, which brings more Facebook users back to the article on your site."[119] Because online publishers generate incremental revenue for each click on an article, more user visits meant more money. According to Facebook, installation of social plugins increased traffic on average by 200%.[120]

Thousands of publishers (competitors of Facebook for digital ad dollars), and other websites and apps, hoping for incremental ad revenue, flocked to install the Facebook Like button. All a third-party had to do was install a single line of HTML Facebook code into their application.[121] Within the first week of availability, more than 50,000 sites added social

---

[116] John D. Sutter, *Facebook Makes It Easier for Users to Share Interests Across Web*, CNN.COM (April 21, 2010), http://www.cnn.com/2010/TECH/04/21/facebook.changes.f8/index.html. Like buttons are small buttons, which often display the text 'Like' alongside a blue thumbs-up icon. Third-parties could install the buttons on their websites. A news website, for example, might display Like buttons near articles. Readers could click on the button to indicate support for an article's point of view. When clicked, the button counter might increase by one, the user be given an opportunity to comment, and the article be published to the user's News Feed. For users, the Like button was marketed as a communications tool—enabling users to "easily share interesting content with friends." *Facebook Platform Showcase*. FACEBOOK.COM (Dec. 5, 2010), http://developers.facebook.com/showcase/news?p=wallstreetjournal, [https://web.archive.org/web/*/http://developers.facebook.com/showcase/news?p=wallstreetjournal]. *See also Like Button for the Web*, FACEBOOK.COM (2018), https://developers.facebook.com/docs/plugins/like-button.

[117] The Facebook Login plugin (called Registration Plugin at the time) was another plugin launched December 2008 that allowed third-parties to deploy Facebook's user registration and sign-in, as opposed to their own. More seamless sign-in meant more sign-ins, which often meant more revenue. *See* Jessica E. Vascellaro, *Facebook Plans Enhanced Ties to Outside Services*, WALL STREET J. (July 24, 2008), https://www.wsj.com/articles/SB121687251639480377?mod=searchresults&page=1&pos=17.

[118] *See The Value of a Liker*. FACEBOOK.COM (Sept. 29, 2010), https://www.facebook.com/notes/facebook-media/value-of-a-liker/150630338305797.

[119] *Id.*

[120] *See Facebook Platform Showcase*, *supra* note 116.

[121] *See generally Brand Permissions Center Usage Guidelines*, FACEBOOK.COM (Dec. 9, 2010), http://www.facebook.com/brandpermissions/logos.php [https://web.archive.org/web/20101209212738/http://www.facebook.com/brandpermissions/logos.php]; *Social*

plugins.[122] CNN, The New York Times, The Wall Street Journal, Slate, and ABC were among the many initial adopters.

Facebook social plugins opened a vulnerability between users' devices and Facebook's servers much in the same way that Beacon did a few years earlier. Like Beacon, social plugins required independent businesses to install Facebook code on their websites, which opened a backdoor communication between users' devices and Facebook's servers. Meaning, the Like button was not simply a static image that one hard-coded into their website. If The New York Times had installed Like buttons, and the user visited nytimes.com, while the user initiated an HTTP request with a Times server, the nytimes.com response would include Facebook code that would then automatically initiate a separate request from the user to Facebook—for the purpose of retrieving and displaying a Like button. As was the case with Beacon, if it so wanted, Facebook could leverage third-party initiated requests to glean users' data, and to write and/or read tracking cookies.[123]

For many years, Facebook perpetuated the belief it would not leverage backdoor access, the way it had with Beacon, to conduct surveillance for commercial purposes. Consumers had shown an aversion to the idea of Facebook tracking them while not on Facebook. The steady stream of public claims that Facebook did not and would not use the network of code for social plugins to monitor and track consumer behavior prompted consumers to continue to trust and

---

Plugins, FACEBOOK.COM (Nov. 26, 2010), http://developers.facebook.com/docs/reference/plugins/like [https://web.archive.org/web/20101126215652/http://developers.facebook.com/docs/reference/plugins/like]; *Social Plugins*, FACEBOOK.COM (Dec. 7, 2010), http://developers.facebook.com/plugins [https://web.archive.org/web/20101207235101/http://developers.facebook.com/plugins].

[122] *How to Use the New Facebook Social Plugins for Your Business*, FACEBOOK.COM (May 4, 2010), https://www.facebook.com/notes/facebook-for-developers/how-to-use-the-new-facebook-social-plugins-for-your-business/394310302301/.

[123] Cookies set during the retrieval of third-party functionality are called third-party cookies (or TPCs). For a definitional break-down of third-party cookies, first-party cookies, and session cookies, see Jessica Davies, *Know Your Cookies: A Guide to Internet Ad Trackers*, DIGIDAY.COM (Nov. 1, 2017), https://digiday.com/media/know-cookies-guide-internet-ad-trackers/.

therefore choose Facebook over alternatives in the market. But Facebook's claims were also important in soliciting the coordination of third-parties to spread the presence of Facebook code across the internet. Many third-parties, publishers for example, competed with Facebook on the advertising side of the market. They licensed and installed social plugins as a means to distribute their own content. Surveillance of their own readers, however, could be used against them to undercut the value of and pricing power over their own proprietary readers.[124] Specifically, if Facebook could compile a list of people that read the *Journal*, even those who did not use Facebook, it could simply sell the ability to retarget "*Journal* readers" with ads across the internet for a fraction of the cost that the *Journal* charged.

When Zuckerberg first announced the Like buttons at the 2010 developer's conference, he did not mention that Like buttons could be used to track users.[125] At the time, Facebook was under intense privacy scrutiny, some politicians threatened investigations, and Facebook faced competition over privacy. MySpace announced it was now offering superior privacy controls in an attempt to get privacy-concerned users to switch. Facebook was on a pre-IPO mission to get users to choose Facebook over alternatives in the market, and in May 2010, Zuckerberg convened a press conference to address privacy concerns.[126] The consumer technology

---

[124] Facebook surveillance of users on independent publisher sites and apps benefits Facebook advertising revenue in two ways. One, Facebook can leverage the data to better target users (or conduct superior attribution for) on Facebook's own properties. Two, Facebook can leverage the data to directly target a publisher's readers and price undercut a publisher's ad rates.

[125] *See generally* Declan McCullagh, *Facebook 'Like' Button Draws Privacy Scrutiny*, CNET.COM (June 2, 2010), https://www.cnet.com/news/facebook-like-button-draws-privacy-scrutiny/.

[126] On May 26, 2010, Facebook convened a press conference at its Palo Alto headquarter. There, in response to Julia Boorstin, CNBC: How does this controversy and your new approach to privacy affect your approach to revenue and your business model?, Zuckerberg said: "So it might be kind of crazy... to people...I don't know. It might seem weird. I don't actually know exactly what the external perception of this is. But I always read these articles that are like "OK you guys must be doing this because it's going to make you more money." And honestly for people inside the company that could not ring less true." KIRKPATRICK, *supra* note 39; Jessica E. Vascellaro, *Facebook Grapples with Privacy Issues*, WALL STREET J. (May 19, 2010), https://www.wsj.com/articles/SB10001424052748704912004575252723109845974. U.S. senators Charles Schumer (D-N.Y.), Michael Bennet (D-Col.), Mark Begich (Alaska) and Al Franken (D-Minn.) wrote an open letter to Facebook founder and CEO Mark Zuckerberg addressing privacy concerns. *See generally* Senators' Letter to Facebook, POLITICO (Apr. 27, 2010), https://www.politico.com/story/2010/04/senators-letter-to-facebook-036406.

publication *CNET* covered Facebook's Like button launch and addressed users' concerns around Like buttons being used to decrease user privacy.[127] One issue, even absent the topic of cookies, was that the presence of Like buttons on other sites enabled Facebook to receive any internet users' URLs as they moved around the internet, and Facebook's privacy policy did not appear to obtain users' consent for this practice.[128] Facebook responded by saying that its privacy statement was "not as clear as it should be, and we'll fix that."[129] Barry Schnitt, a Facebook spokesman, then allayed concerns by explaining that Facebook plug-ins work like any other plug-ins on the internet, Facebook does not use social plug-in data for advertising, and Facebook may use received data to catch bugs in its software.[130]

But in November of 2011, Dutch researcher Arnold Roosendaal exposed Facebook's hidden activity with Like buttons in the way that Berteau did earlier with Beacon. Shortly after launching the Like buttons, Roosendaal published a paper showing that Facebook was using the Like button code now installed on third-party sites to write and read user cookies.[131] Roosendaal showed that each time a Facebook user visited a site with a Like button, Facebook retrieved the user's Facebook website login cookies, which contained the user's unique identifying number, traceable to his or her real identity.[132] Facebook again was leveraging login cookies from the communications network to conduct detailed surveillance possibly for the advertising side of its business. In addition to a user's ID number, Facebook retrieved the specific URL the user was on, which revealed the title of an article the user was reading or the name of the product a user

---

[127] McCullagh, *supra*, note 125.

[128] *Id*. (for example, CNET pointed out that Facebook's FAQ stated, "No data is shared about you when you see a social plug-in on an external website," and that Facebook's privacy policy also did not appear to obtain users' consent.)

[129] *Id*.

[130] *Id*.

[131] Arnold Roosendaal, *Facebook Tracks and Traces Everyone: Like This!*, (Tilburg L. Sch. Legal Studs. Res. Paper Ser. No. 03/2011, Nov. 30, 2010), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717563.

[132] *Id*.

was buying. Roosendaal then demonstrated that Facebook used these open connections to write cookies and surveil the behavior of people that did not even have Facebook accounts.

The *Wall Street Journal* published the results of its own investigative study confirming Roosendaal's findings.[133] The study, led by a former Google engineer, examined the presence of social widgets on the world's top 1,000 most-visited sites. The *Journal* concluded that Facebook buttons had been added to millions of websites, including a third of the top 1,000 most-visited sites. Facebook knew when a user reads an article about "filing for bankruptcy" on MSNBC.com or about depression on a small blog, even if the user didn't click any Like button.

With a finger on the pulse of Americans' sentiment towards tracking, the *Journal* recommended users log-out of Facebook to stop Facebook from tracking them and gave Facebook an opportunity to comment. Bret Taylor, Facebook's chief technology officer at the time, responded definitively to the privacy breach allegations, "We don't use them for tracking and they're not intended for tracking."[134] Taylor clarified that Facebook places cookies on the computers of people that visit facebook.com to protect users' Facebook accounts from cyber-attacks.[135] The Journal also gave Facebook an opportunity to answer to Roosendaal's allegation that Facebook was tracking people that did not even have a Facebook account. Facebook said that Roosendaal had found a "bug," and that it had therefore discontinued this practice.[136]

But the issue—as important as it was—was not put to rest. Later that year, in September of 2011, Nik Cubrilovic, an Australian internet security contractor, followed up on Roosendaal's

---

[133] Amir Efrati, *'Like' Button Follows Web Users*, WALL STREET J. (May 18, 2011), https://www.wsj.com/articles/SB10001424052748704281504576329441432995616 (The WSJ study also found that Facebook trackers could continue to track internet users even if users had closed their browsers or turned off their computers.). *See also* Reed Albergotti, *Facebook to Target Ads Based on Web Browsing*, WALL STREET J. (June 12, 2014), www.wsj.com/articles/facebook-to-give-advertisers-data-about-users-web-browsing-1402561120.

[134] Efrati, *supra* note 133.

[135] *Id*.

[136] *Id*.

and the *Journal's* discoveries, and published an article showing that Facebook Like and other plugins were *still* tracking user activity outside of Facebook even if users had completely logged out of Facebook.[137] Normally, when a user logs out of a service, the service's login cookies terminate. But Facebook's cookies weren't terminating, they were persistent and still able to identify and track people. Mainstream media picked up on Cubrilovic's reporting in an effort to hold Facebook accountable. In coverage about Facebook's "alleged cookie snooping," the *Huffington Post* asked, "Is Facebook tracking which websites users visit even after they've logged out of the service?"[138]

Facebook again acted quickly to pacify the growing drumbeat of public concern over Facebook's intentions with regards to leveraging social plugin code for surveillance. A Facebook spokesperson, Facebook engineers, and the Facebook privacy policy were put forth to dispel worry. In one instance, Facebook responded to a CBS News inquiry with a statement that, "Facebook does not track users across the web. … No information we receive when you see a social plugin is used to target ads, [and] we delete or anonymize this information within 90 days ...."[139] Elsewhere, Facebook engineers responded directly in the comments section of blogs and articles.[140] Facebook engineer Arturo Bejar pleaded with users, "please know that ... when you're logged in (or out) we don't use our cookies to track you on social plugins to target ads or sell your information … We use your logged in cookies ... for safety and protection."[141] When

---

[137] *See* Jason O. Gilbert, *Facebook Logout Tracking: Privacy Concerns Arise Over Alleged Cookie Snooping*, HUFFINGTON POST (Sept. 26, 2011), https://www.huffingtonpost.com/2011/09/26/facebook-logout-cookies-privacy-tracking_n_980838.html. S*ee also* Emil Protalinski, *Facebook Denies Cookie Tracking Allegations*, ZDNET.COM (Sept. 25, 2011), https://www.zdnet.com/article/facebook-denies-cookie-tracking-allegations/.

[138] Gilbert, *supra* note 137.

[139] Erik Sherman, *Facebook's New Privacy Bust: Users Log In but They Can't Log Out,* CBS NEWS (Sept. 26, 2011), https://www.cbsnews.com/news/facebooks-new-privacy-bust-users-log-in-but-they-cant-log-out-update/.

[140] *See* Protalinski, *supra* note 137 (Facebook spokesperson replied to a journalist's request for comment by pointing to Facebook engineer's public blog comments).

[141] *Id*.

pressed by news outlet *ZDNet* for an official statement, a Facebook spokesperson directed the reporter to Bejar's statement.[142] The *New York Times* also disseminated Facebook's representations to the public.[143] This all appeared to corroborate what the Facebook Help Center represented to consumers at the time, "we do not use [information we see when you visit a website] to deliver ads."[144]

Facebook's reasoning though—regarding users' safety and protection—still called into question why Facebook cookies contained users' Facebook ID numbers. Normally, a company might include user ID numbers in cookies if it intended to conduct individual tracking. Thus, in direct response to Cubrilovic's allegations, Facebook promised to change how its cookies worked so that users' ID numbers were not embedded in cookies after users logged out.[145] The removal of account ID numbers from cookies ensured that Facebook could not conduct de-anonymized user surveillance in spite of claims of its intentions not to do so.

If Facebook, or any other company, did want to conduct mass commercial surveillance on users, one precondition would be the pervasive consent and coordination of third-parties (e.g., *The New York Times* and Overstock). One way a company could do this would be to do so overtly, as Facebook had with Beacon—simply ask users with a pop-up box if they want to share what they are reading or buying on other sites with Facebook. But this direct, overt, attempt at getting users to share their information had failed. Another way Facebook could go about accomplishing the same end would be to get third-parties to install Facebook code for an

---

[142] *Id*.

[143] Riva Richmond, *As 'Like' Buttons Spread, So Do Facebook's Tentacles*, N.Y. TIMES (Sept. 27, 2011), https://bits.blogs.nytimes.com/2011/09/27/as-like-buttons-spread-so-do-facebooks-tentacles/.

[144] *See* Protalinski, *supra* note 137.

[145] *See* Alan Henry, *Facebook Is Tracking Your Every Move on the Web; Here's How to Stop It,* LIFEHACKER.COM (Sept. 26, 2011), https://lifehacker.com/5843969/facebook-is-tracking-your-every-move-on-the-web-heres-how-to-stop-it.

independent product, like the Like buttons, then eventually leverage use and dependence of Like buttons (or other social plugins) to later extract a new use permission.

For the American consumer, this architecture of interests in the market was precarious. Independent businesses were creating consumer privacy vulnerabilities for their own financial gain; and, it all rested on Facebook living up to its word. This fact did not wash over the reporters that sought to hold Facebook accountable to its representations. In December of 2012, The *Wall Street Journal* revisited the issue, to point out that Facebook plugins now appeared on *two-thirds* of websites surveyed.[146] But Facebook again publicly assured that it only uses data from unchecked Like buttons for security purposes and to fix bugs in its software. Noticeably absent from Facebook's public statement was the fact that Facebook also filed a patent application the year prior, on September 22, 2011, for a "method … for tracking information about the activities of users of a social networking system while on another domain."[147] Michael Arrington, veteran tech blogger, caught it and called it "Brutal Dishonesty."[148]

If Facebook wanted to eventually usurp privacy by using the back-end code from Like buttons or other social plugins, it faced a roadblock—the user referendum process for privacy changes introduced a few years earlier. Thus, while publicly representing that it only used social plugin data for users' safety and protection and generally deflecting concern over Facebook intentions, Facebook simultaneously dismantled the user voting process. In late 2012, with over a billion users, and an historic initial public offering now under its belt, Facebook addressed this roadblock expediently. Facebook proposed major changes that could pave the way for Facebook

---

[146] *See* Julia Angwin, *It's Complicated: Facebook's History of Tracking You,* PROPUBLICA.ORG (June 17, 2014), https://www.propublica.org/article/its-complicated-facebooks-history-of-tracking-you; Geoffrey A. Fowler, *What You Can Do About Facebook Tracking*, WALL STREET J. (Aug. 5, 2014), https://www.wsj.com/articles/what-you-can-do-about-facebook-tracking-1407263246.

[147] U.S. Patent No. 2011/0231240A1 (filed Feb. 8, 2011) (issued Sept. 22, 2011).

[148] Michael Arrington, *Facebook: Brutal Dishonesty*, UNCRUNCHED.COM (Oct. 1, 2011), https://uncrunched.com/2011/10/01/brutal-dishonesty/.

to decrease user privacy. One provision proposed was the abolishment altogether of future referendums for privacy changes.[149] After soliciting user feedback, and receiving push-back, Facebook submitted the proposed changes to a vote. Eighty-eight percent of users voted against Facebook's proposed privacy changes.[150]

But Facebook shrugged. At this point, users had high switching costs and the fine print of the governing documents requiring referendums had a kill switch. In order for a user vote to be binding, 30% of users would have had to vote in the election.[151] With over a billion users, and only some 589,000 votes casted, Facebook discarded the results of the election.[152] Facebook then moved forward with privacy erosions and the abolishment of the referendum process. Many users protested that Facebook had not informed them of the upcoming election, either by notifying them upon a Facebook login or by simply sending them an email.[153] Other users claimed to receive an email notifying them of a vote, but not informing them how and where to vote. It was an election where Facebook didn't want anyone voting.

C. POST-POWER: Deterioration of the Promise Not to Track

*"We give lots of f*** about your privacy, so we wrote this. Read it, so you know what the f*** we're going to do with the s*** you post ..."*

—Comments by Facebook employees in 2011 parodying the genuineness of Facebook's concern for user privacy; specifically, the Facebook user privacy policy.[154]

---

[149] *See* ANTONIO GARCIA MARTINEZ, CHAOS MONKEYS: OBSCENE FORTUNE AND RANDOM FAILURE IN SILICON VALLEY (2016).

[150] *See* Dan Farber, *The Facebook Vote and a Nation-State in Cyberspace*, CNET.COM (Dec. 11, 2012), https://www.cnet.com/news/the-facebook-vote-and-a-nation-state-in-cyberspace/#.

[151] *Id*.

[152] *Id*.

[153] *See* Donna Tam, *The Polls Close at Facebook for the Last Time*, CNET.COM (Dec. 10, 2012), https://www.cnet.com/news/the-polls-close-at-facebook-for-the-last-time/.

[154] *See* Alexia Tsotsis, *It's About Time Someone Translated the Facebook TOS Into Bro Speak*, TECHCRUNCH.COM (Aug. 17, 2011), https://techcrunch.com/2011/08/16/code-curls-girls/; Martinez, *supra* note 149 at 317.

By early 2014, rivals that initially competed with Facebook including MySpace, Friendster, Mixi, Cyworld, hi5, BlackPlanet, Yahoo's 360, AOL's Bebo, and dozens of others, had exited the market.[155] Google—Facebook's rival and nemesis—announced it would shut down its competitive social network Orkut. By June of 2014, Orkut had exited the market, effectively ceding the social media market to Facebook.[156] For Facebook, the network effects of over a billion users on a closed communications protocol further locked-in the market in its favor. With countless friends and family connected to a given consumer, the cost of foregoing Facebook for the consumer grew in proportion with Facebook's growth. For Facebook, these circumstances—the exit of competition and the lock-in of consumers—greenlit a change in conduct.

Facebook's monopoly power gave it the ability to further deteriorate privacy and extract more of the user's data—which, as Dave Wehner, chief financial officer of Facebook, clarified on Facebook's Q2 2018 earnings call, is directly correlated with higher ad revenues.[157] Part I of this Paper detailed Facebook's initial commitment to privacy, and Sections A and B surveyed Facebook's inability to extract a condition of surveillance in a competitive market. Section C traces Facebook's ability to reverse course post-power—direct evidence of monopoly power. First, Facebook initiates user surveillance for commercial ad purposes. Second, Facebook ties user identification with cookies to conduct more intrusive surveillance. Third, Facebook then circumvents user attempts to opt-out or block Facebook's quality degradations. The three quality deteriorations can be understood as the monopoly rents Facebook is able to command in the market today. Absent competition, Facebook is able to degrade quality levels below that which was required in a competitive market, and financially profit from this conduct.

---

[155] *See supra* text accompanying notes 69-70.
[156] *See* Huet, *supra* note 76.
[157] *Facebook Q2 Earnings*, *supra* note 12.

Facebook's quality deterioration led to an interesting phenomenon—decreasing user satisfaction, despite Facebook's continued ability to retain and grow its user base. According to the American Consumer Satisfaction Index (ASCI), social media is amongst the lowest scoring of all industries surveyed. With an industry average of 72, social media's ASCI score is lower than even health insurance and airlines.[158] Facebook, with a score of 67, and a trailing average of 66, has an ASCI score lower than almost every American airline—and is also lower than the average industry benchmarks of 95% of the industries covered by the ASCI study. This paradox defies the law of demand—which says that given a constant price, a decrease in quality must necessarily lead to a decrease in buyer consumption.

1. Facebook Initiates Commercial Surveillance.— In June of 2014, Facebook announced it would leverage its code presence on third-party applications to track consumers, enabling it to surveil the specific online behavior of this country's citizens despite widespread preference to the contrary.[159] Facebook would do precisely what it had spent seven years promising it did not and would not do, and finally accomplished what the previous competitive market had restrained it from doing. With a relatively quick software update, Facebook would leverage the code on third-party sites and apps used to deliver other Facebook products—Like buttons, Login buttons, conversion tracking pixels,[160] retargeting pixels, and the Facebook software development kit—

[158] *ACSI E-Business Report 2018*, THEACSI.ORG (July 24, 2018), http://www.theacsi.org/news-and-resources/customer-satisfaction-reports/reports-2018/acsi-e-business-report-2018.

[159] *Making Ads Better and Giving People More Control Over the Ads They See*, NEWSROOM.FB.COM (June 12, 2014), https://newsroom.fb.com/news/2014/06/making-ads-better-and-giving-people-more-control-over-the-ads-they-see/; Albergotti *supra* note 133. For a technical description of how Facebook tracks people, reference a technical report prepared for the Belgian Privacy Commission in 2015: GÜNEŞ ACAR, BRENDAN VAN ALSENOY, FRANK PIESSENS, CLAUDIA DIAZ, & BART PRENEEL, FACEBOOK TRACKING THROUGH SOCIAL PLUG-INS, https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf.

[160] The Facebook conversion tracking pixel is a piece of Facebook code that advertisers affix to their websites to enable Facebook to report back to the advertisers whether a Facebook ad campaign is yielding traffic and sales; in other words, it a piece of code that allows the advertiser to measure the return-on-investment of Facebook ad

for the additional new purpose of tracking users.[161] In a previously competitive market, Facebook was not able to get away with this qualitative degradation. Now Facebook could significantly degrade its quality because consumers no longer had alternative social networks to turn to.

Facebook had repeatedly pacified privacy concerns by representing that any data gleaned from the presence of Facebook code on third-party sites was not to be used for "commercial purposes" but rather for users' own "safety and protection." But now Facebook changed course and announced that the data derived from tracking consumers would augment Facebook ad targeting, attribution, and measurement.[162] In other words, this deterioration of privacy would be directly related to increased revenue and profits. First, Facebook would use data from this commercial surveillance to enhance its ad targeting algorithms, which meant that Facebook ads could be more targeted and reach a larger relevant advertising base than those of other ad sellers in the market—such as The New York Times or Hearst. Second, data from commercial surveillance would allow Facebook to get paid for more advertising through increased attribution. A significant percentage of marketers only pay Facebook if ads result in a specific measurable outcome (*i.e.*, a click on an ad or a sale of a product). Facebook calls these action-based ads. Attribution refers to the process of identifying the set of user actions that lead to a

---

campaigns. The announcement that Facebook would use data it retrieves from its conversion tracking pixels also upset advertisers. The tracking pixel was there to report to the paying advertiser whether the ads were working. Now, Facebook could use data garnered from one campaign to sell advertising to competitors. For example, Facebook could use data from the Facebook conversion tracking pixels on Audi's website (to measure Audi's ad campaign), to better sell advertising to Mercedes (by targeting users who previously looked at Audis on Audi's website).

[161] *See* Cotton Delo, *Facebook to Use Web Browsing History for Ad Targeting*, ADAGE.COM (June 12, 2014), adage.com/article/digital/facebook-web-browsing-history-ad-targeting/293656/.

[162] *See id.* (Facebook is using the passive data, where users go on their PCs and phones, to make its own ads smarter). *See also,* Parmy Olson, *Facebook Moves to Become the World's Most Powerful Data Broker*, FORBES MAGAZINE (April 30, 2014), https://www.forbes.com/sites/parmyolson/2014/04/30/facebok-moves-to-become-the-worlds-most-powerful-data-broker/#662d16f42006 (Facebook uses personal data as "leverage with advertisers who are desperate to better-target their ads").

desired result.[163] Increased commercial surveillance allows Facebook to fine-tune attribution models and claim credit for more actions, which further increases Facebook's ad revenues.

When Facebook reversed course in 2014, unlike when it tried to do so earlier, Facebook code was deployed across millions of sites and mobile apps, and the intentions of the code were altered in one fell swoop. Over the course of the seven years that Facebook represented it would not use social widgets to track consumers, millions of websites had signed up for and installed Facebook plugins.[164] Not including mobile apps, this included approximately 30% of the top 1 million of the most-visited websites,[165] including news websites like The Wall Street Journal, The Washington Post, and The San Francisco Chronicle. Facebook laid the groundwork for tracking by requiring third-parties to install Facebook code in order to license Facebook's other products. For independent publishers and retailers, Facebook would thereafter tie surveillance of their own customers with the continued use and license of Facebook's social network products for businesses.

Proprietary access to subscribers and the identities of readers and visitors is a highly guarded asset historically by subscription businesses. It is unlikely that publishers would have shared this information unless they were under the belief that Facebook was a content distribution platform and traffic generator, not a surreptitious aggregator of consumer data for Facebook's own internal, and competitive, advertising sales efforts. Facebook obtained the initial cooperation of third-party businesses through the inducements of content distribution and the convenience of single login. Now Facebook would receive the ability to monitor the behavior of *their* customers—competitors with Facebook in the digital advertising market—by changing the

---

[163] *IAB Attribution Hub*, IAB.COM (2018), https://www.iab.com/guidelines/iab-attribution-hub/.

[164] *See* BUILTWITH.COM*, supra note 6.*

[165] *See* Steven Englehardt & Arvind Narayanan, *Online Tracking: A 1-million-site Measurement and Analysis*, WEBTAP.PRINCETON.EDU (2018), http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf.

fine print of permissions. Facebook increasingly knew as much about The Wall Street Journal's readers as the Journal did itself. Furthermore, unlike the Journal, Facebook now knew which Journal readers were avid ESPN readers, giving it the capability to bundle and sell targeted audiences, which further commoditized the value of competitors' inventory. Under the new regime, when a consumer visited a website with a Facebook plugin, Facebook piggy-backed onto the requests and responses necessary to simply display the plugins, to now also surveil the users of competitor ad sellers—rendering the Facebook code a Trojan Horse of sorts.

From the consumer's perspective, consumers could choose whether to reveal information on Facebook itself, and they did.[166] Now, consumer choice, even the choice not to use Facebook, no longer mattered. In the earlier competitive market, the cooperation of third-parties, on which Facebook's tracking depended, was predicated on how consumers felt about the proposition. As discussed above, previously, when consumers protested, participating companies stopped coordinating with Facebook.[167] In 2014, unlike in 2007, Facebook did not have only a handful of third-parties working with it. Facebook had a substantial portion of the horizontal market coordinating with it for some functionality or another—whether for user-registration or article sharing. These independent businesses now had their own switching costs. They had built their businesses over the last seven years to depend on Facebook code, and now, that reliance was correlated with their own revenue performance.[168] Finally, the conscientious objector no longer had any power to alter the direction of the wider market.

Reflecting its ability to influence market actors in the ecosystem, Facebook then required all businesses to change their own privacy policies to extract from their own users the consent to

---

[166] *See* Acquisti & Gross, *Imagined Communities*, *supra* note 50 at 13 (*e.g.*, Acquisti & Gross' study of what Facebook users do to satisfy their desire for privacy revealed that users "claim to manage their privacy fears by controlling the information they reveal").

[167] *See* McCarthy, *supra* note 102.

[168] *See generally* Roosendaal, *supra* note 131; FACEBOOK.COM, *supra* note 118.

have Facebook track them for commercial purposes. For convenience, Facebook provides exact copy-and-paste legal language to use:[169]

> "Third parties, including Facebook, may use cookies, web beacons, and other storage technologies to collect or receive information from your websites, apps and elsewhere on the internet and use that information to provide measurement services, target ads …"

This is how consumers went from having a preference of privacy to having nearly every competitor in the market extract from them identical and uniform consent for Facebook's commercial surveillance practices.

2. Facebook Leverages Consumer Identity for Stronger Surveillance.—Facebook further deteriorated user privacy by tying the newly announced tracking of consumer behavior across the wider internet with the real, stable, human identities that Facebook knew because of its position in the social network market.[170] When the restraining forces of competition worked, Facebook had to remove user IDs from cookies to ensure that Facebook could not conduct de-anonymized

---

[169] *Facebook Platform Policy*, FACEBOOK.COM (2018), https://developers.facebook.com/policy ("Obtain adequate consent from people before using any Facebook technology that allows us to collect and process data about them, including for example, our SDKs and browser pixels. When you use such technology, provide an appropriate disclosure... That third parties, including Facebook, may use cookies, web beacons, and other storage technologies to collect or receive information from your websites, apps and elsewhere on the internet and use that information to provide measurement services, target ads and as described in our Data Policy.").

[170] This decision was reflected in Facebook's re-launch of the Atlas ad server. *See generally* see Jack Marshall, *Adblock Lets Users Quash Facebook's Atlas Tracking*, BLOGS.WSJ.COM (Oct. 1, 2014), https://blogs.wsj.com/cmo/2014/10/01/adblock-lets-users-quash-facebooks-atlas-tracking/?ns=prod/accounts-wsj; Zach Rodgers, *With Atlas Relaunch, Facebook Advances New Cross-Device ID Based on Logged in Users*, ADEXCHANGER.COM (Sept. 28, 2014), https://adexchanger.com/platforms/with-atlas-relaunch-facebook-advances-new-cross-device-id-based-on-logged-in-users/. Also consider comments from competitive ad sellers in the digital media market, for example, from YieldBot CEO Jonathan Mendez, in an interview with The Wall Street Journal, "[Facebook has] a lot of advantages … in terms of their data and relationship with consumers and this allows them to leverage it." *Why You Should Care About Facebook's Atlas Ad Relaunch*, WALL STREET J. (Oct. 15, 2014), https://www.wsj.com/video/why-you-should-care-about-facebooks-atlas-ad-relaunch/C11CF1DC-C0CA-4D0D-8F98-2ACEA86CD0B7.html?mod=searchresults&page=1&pos=3.

surveillance.[171] Now, with the foreclosure of competition, Facebook would reinstate invasive identity monitoring.[172] This reinstatement is further evidence of Facebook's monopolistic market power.[173]

By augmenting tracking with consumer identification, Facebook also circumvented users' attempts to limit tracking by deleting cookies (or resetting a mobile device's advertising identifier). Clearing cookies expunges cookie variables from a user's device and breaks the link between one's device and the cookie's memory.[174] For example, suppose The New York Times wanted to surveil a user via cookie ID 123456789. If a user deleted the cookie, the next time the user visited nytimes.com, the Times' server would try to identify the user but find no cookie. The profile the Times had compiled on user 123456789 would thereafter be worth little. The ability to correlate tracking data to one's identity now circumvented the ability of consumers to wipe

---

[171] *See* Henry, *supra* note 145.

[172] For an advertising competitor's perspective on Facebook's decision to tie Facebook IDs with tracking cookies, see Olson, *supra* note 162 (where Mark DiMassimo, CEO of the ad agency DiMassimo Goldstein, explains "Facebook [now] knows who you are").

[173] Part IV of this paper examines whether Facebook illegally acquired monopoly power in the social network market. A separate issue to be examined is whether, by bundling social network user IDs into its own advertising inventory and the inventory of other market actors like Hearst, Facebook is illegally "leveraging" its monopoly position in the social network market to inappropriately monopolize the advertising market. Though the Supreme Court curtailed Section 2 "leveraging" theory in *Verizon v. Trinko*, some Courts have interpreted *Trinko* to leave the door open to some types of leveraging claims. Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398 (2004); Z-Tel Communications, Inc. v. SBC Communications, Inc., 331 F. Supp. 2d 513 (E.D. Tex. 2004). The Areeda treatise contends the Sherman Act permits "leveraging" claims where (a) a firm uses monopoly power in market A, (b) to place rivals in market B at a competitive disadvantage (by raising B's costs or decreasing the quality of B's product), and (c) higher prices, reduced output, or reduced quality (normally associated with monopoly power) results in market B. In the technical sense, the authors of the Areeda treatise argue that proof of (c) meets the definition of "monopolization" or "attempt to monopolize" within the literal language of §2, that monopoly market share is not necessary to a finding of "monopolization" or "attempt to monopolize", and that therefore, "leveraging" is an unnecessary distinguishable §2 theory. AREEDA & HOVENKAMP, §652, *supra* note 26. Furthermore, Facebook's tracking of consumers on third-party sites and leveraging of user IDs may be challenged as illegally maintaining and perpetuating the Facebook monopoly. New entrants in the social media market that also rely on attracting advertisers cannot compete with Facebook's commercial surveillance. Consider, for example, the fact that Facebook monetizes U.S. & Canada users at a $17.07 average revenue per user (ARPU), but that SnapChat can only monetize North American users at a $1.81 ARPU (even though SnapChat users only spend half the amount of time on SnapChat than they do on Facebook). See Alexei Oreskovic, *Look at the Big Gap Between SnapChat's Revenue Per User and Facebook's*, BUSINESSINSIDER.COM (May 10, 2017), https://www.businessinsider.com/snapchat-arpu-versus-facebook-arpu-charts-2017-5.

[174] *See* Chris Jay Hoofnagle, Ashkan Soltani, Nathaniel Good, & Dietrich J. Wambach, *Behavioral Advertising: The Offer You Can't Refuse*, 6 HARV. L. & POL. REV. 273, 277 (2012).

their slate clean—Facebook, unlike The New York Times, could immediately match observed behavior with a stable identity. The social network had a real-name policy, and occasionally required users to prove their names with state-issued identification.[175] To Facebook, it was not user 123456789 that was reading Coming Out to Your Wife, it was simply Jacob Greenberg. If the user deleted Facebook cookies, the profile Facebook had compiled could still live on under the user's real-name profile. Furthermore, Facebook could re-cookie a user the next time the user visited the Facebook social network, which users did multiple times per day.

With code that used a persistent singular identification mechanism now pervasive across competing websites and apps, Facebook could connect the dots on consumers as they moved from site to site, and from computer to mobile phone, to compile rich dossiers on users. Facebook was the single eye that could see what John Doe was doing on both The New York Times and on The Wall Street Journal.[176] The competitive market once ensured that competitors on the advertising side of the business did not track and monitor what users were doing across the horizontal market. The unique ability to conduct horizontal surveillance, for both Facebook and Google, explains the current duopoly in digital advertising, where nearly all industry growth goes to only two companies. Both companies, however, only achieve this end by leveraging a monopoly position in another market—for Facebook, the social network market, and for Google, the search market.

---

[175] For Facebook's name policy, *see What Names Are Allowed on Facebook?*, FACEBOOK.COM, https://www.facebook.com/help/112146705538576 (stating that "The name on your profile should be the name that your friends call you in everyday life. This name should also appear on an ID or document from our ID list."). Sometimes, Facebook has required users to prove their identity by submitting a copy of government-issued identification. *See*, *e.g.*, Hamm Samwich, *A Drag Queen's Open Letter to Facebook*, HUFFINGTON POST (Sept. 18, 2014), https://www.huffingtonpost.com/hamm-samwich/nominative-dysphoria-a-dr_b_5839148.html.

[176] *See generally* Rodgers, *supra* note 170 (explaining that the Facebook ID, uses the "login" as the "foundation" of tracking, measurement, and ad personalization).

Armed with data derived from Facebook's new surveillance capabilities, Facebook could bill advertisers for more conversions, and sell advertising based on surveillance data.[177] For example, if Sally Smith read on the family's shared computer an article about marital problems on a small hometown news site, Facebook could know and save it to Smith's dossier. When Smith wakes up the next morning refreshed from a night's sleep, the marital drama now tucked in the past, and logs onto Facebook, she might now be presented with an ad from a divorce lawyer in her Facebook News Feed. Alternatively, her husband might have woken up, logged opened ESPN on the same computer, and himself been presented with an ad for a divorce lawyer. Behind the scenes in both cases, Facebook data derived from Facebook surveillance is the facilitator.

3. Facebook Circumvents Consumer Attempts to Opt-Out.—Consumers did not want Facebook to track their behavior across the Internet,[178] so they tried to circumvent Facebook's new quality deteriorations. On the one hand, this consumer behavior is further evidence of users' preference for no surveillance. On the other, Facebook's behavior is evidence of Facebook using its market power to forcibly impose on consumers that which they are still—in a consolidated market—trying to resist. First, Facebook itself did not and does not allow consumers to opt-out of the new off-site tracking. Second, Facebook chose to ignore consumers' explicit requests,

---

[177] *See* Delo, *supra* note 161.

[178] *See* C. J. Hoofnagle, J. M. Urban, and S. Li, *Privacy and Modern Advertising: Most US Internet Users Want 'Do Not Track' to Stop Collection of Data about their Online Activities*, AMSTERDAM PRIVACY CONF. (Oct. 2012); Lymari Morales, *U.S. Internet Users Ready to Limit Online Tracking for Ads*, NEWS.GALLUP.COM (Dec. 21, 2010), https://news.gallup.com/poll/145337/internet-users-ready-limit-online-tracking-ads.aspx; Kristen Purcell, Joanna Brenner, & Lee Rainie, *Search Engine Results 2012*, PEW RESEARCH CENTER, http://www.pewinternet.org/2012/03/09/search-engine-use-2012/; TRUSTE AND HARRIS INTERACTIVE, *Privacy And Online Behavioral Advertising*, TRUSTE.COM (July 2012), http://truste.com/ad-privacy/TRUSTe-2011-ConsumerBehavioral-Advertising-Survey-Results.pdf; J. Turow, J. King, C. J. Hoofnagle, A. Bleakley, & M. Hennessy, *Americans Reject Tailored Advertising and Three Activities That Enable It*, UNIV. OF PENN. SCHOLARLY COMMONS (Sept. 2009), https://repository.upenn.edu/cgi/viewcontent.cgi?article=1138&context=asc_papers.

enacted via the browsers' Do No Track option, to not be tracked. Third, when consumers installed ad blockers to circumvent tracking and targeted advertising, Facebook responded by circumventing the users' installed ad blockers.

First, Facebook did not give users the option to opt-out of Facebook's tracking and monitoring of their online behavior.[179] Instead, Facebook informed users they could stop Facebook from showing them ads based on this new surveillance data by opting out on the Digital Advertising Alliance (or DAA) website. The DAA is an industry alliance formed in response to FTC investigations into the industry's privacy practices and reflects an industry effort to police itself. The DAA's stated mission is to give consumers the choice to opt out of behaviorally targeted advertising.[180] Facebook, Google and others are alliance members. On the DAA's website, the opt-out process was, conveniently, painstakingly inconvenient—the user had to go through a multiple-step process for each Facebook account, browser, and device in each household. One might recall the inconvenience consumers faced opting out of direct marketing calls before adoption of the Do Not Call list. For a household of three, opting out required going through the opt-out process about nine times—*just* for Facebook.[181] If the consumer did go through the DAA's opt-out process, the DAA website often informed the consumer that the opt-out requests "were not completed. This may be the result of a temporary technical issue."[182] Furthermore, the DAA's opt-out solution only worked if a consumer set her browser security settings to *permit* third-party cookies—the very mechanism that allows companies like Facebook

---

[179] *See* Angwin, *supra* note 146.

[180] *See* DIGITAL ADVERTISING ALLIANCE, https://digitaladvertisingalliance.org (last visited Jan. 21, 2019).

[181] Assuming 3 configurations per person (for example, 2 browsers & 1 mobile device).

[182] This has been my experience as a consumer from 2016 to today. My request to opt-out has resulted in an error message stating that the DAA could not process my request. When I try to opt out of Facebook tracking, the DAA presents the following message: "Opt-out requests for 1 participating companies were not completed. This may be the result of a temporary technical issue. Select "Try Again" to request opt outs from those companies again. Click "Understand Your Choices" for more information." *See DAA Webchoices Browser Check*, DIGITAL ADVERTISING ALLIANCE, http://optout.aboutads.info/?c=2&lang=EN (accessed Sept. 2, 2018).

to do what the consumer was now trying to avoid.[183] Almost to the point of comedy, the DAA's website then informed users that if they cleared their cookies (to rid tracking cookies), doing so would inadvertently have the effect of allowing Facebook to track them all over again.[184] Even if the consumer succeeding at opting out, he only opted out of being shown targeted advertising, not of Facebook surveillance.

Second, Facebook also circumvented those users who had explicitly set their browser privacy settings to Do Not Track. Since the DAA's solution did not provide users with meaningful choice, many users instead activated the Do Not Track settings in their web browsers. The Do Not Track setting in browsers was another industry response to threatened regulatory action. Back in 2010, the FTC toyed with the idea of creating a singular national "Do Not Track" list for digital advertising companies, to parallel the Do Not Call list for telemarketers. Such a Do Not Track list would have given consumers a "kill switch," which would turn off tracking across the horizontal market.[185] In an effort to ward off regulation, various industry players promised to give users Do Not Track opt-outs. Microsoft updated the Internet Explorer browser to provide users with a Do Not Track setting. Other browsers—Firefox, Safari, Opera, and Chrome—also adopted the Do Not Track protocol.[186] With Safari, for example, a user could go to Preferences Settings, toggle to the Privacy tab, then select the checkbox "Ask websites not to track me."[187] The Do Not Track protocol though didn't

---

[183] *See id*.

[184] *Id*.

[185] *See* Kenneth Corbin, *FTC Mulls Browser-Based Block for Online Ads*, INTERNETNEWS.COM (July 28, 2010), http://www.internetnews.com/ec-news/article.php/3895496/FTC+Mulls+BrowserBased+Block+for+Online+Ads.htm.

[186] TRACKING PROTECTION WORKING GROUP, https://www.w3.org/2011/tracking-protection/ (controls and issues the protocol); Emil Protalinski, *Everything You Need to Know About Do Not Track: Microsoft vs Google & Mozilla*, THE NEXT WEB (Nov. 25, 2012) https://thenextweb.com/apps/2012/11/25/everything-you-need-to-know-about-do-not-track-currently-featuring-microsoft-vs-google-and-mozilla/ (listing the browsers that have adopted the protocol).

[187] Safari Privacy Settings (Open Safari application; then open "Preferences" from the menu bar; then enter the "Privacy" settings; then check the "Ask websites not to track me" box).

technically block companies from tracking users. Rather, a user's browser would simply send a message notifying companies that he or she does not wish to be tracked.[188] It was simply a polite request, which a company could choose whether or not to heed.

In another demonstration of market power, Facebook would ignore users' activation of Do No Track.[189] In 2013, Erin Egan, the chief privacy officer of Facebook, explained that Facebook would bypass consumer Do Not Track settings because Facebook does not track consumers for advertising purposes, in effect arguing that consumers do not understand what Do Not Track means. [190] "We don't use that data for an advertising purpose," she emphasized. In 2014, after Facebook changed course and began tracking consumers for commercial purposes, Facebook simply continued to ignore consumers' Do Not Track signals.

Sensing rising consumer frustration, the private market responded with software that consumers could use to both stop surveillance and block targeted ads from loading on pages altogether.[191] Ad blockers prevented not only the visual display of advertising, but also third-party tracking. Generally, this worked by blocking the user's device from making third-party initiated HTTP requests with advertising companies. In the Fall of 2014, after Facebook's new tracking announcements, online searches for "how to block ads" spiked at an unprecedented

---

[188] *Id*.

[189] *See generally* Liam Tung, *Google, Facebook 'Do Not Track' Requests? FCC Says They Can Keep Ignoring Them*, ZDNET.COM (Nov. 9, 2015), https://www.zdnet.com/article/google-facebook-do-not-track-requests-fcc-says-they-can-keep-ignoring-them/.

[190] Elise Ackerman, *Google And Facebook Ignore "Do Not Track" Requests, Claim They Confuse Consumers*, FORBES MAGAZINE (Feb. 27, 2013), https://www.forbes.com/sites/eliseackerman/2013/02/27/big-internet-companies-struggle-over-proper-response-to-consumers-do-not-track-requests/#a99039822fc.1.

[191] Common ad blockers work by communications blocking, where the client's request to an ad servers or ad company is prevented from occurring. They can also work by element hiding, where HTML elements are loaded onto the client's page but hidden from the user (for example, hide elements with class = "Ad"). Disconnect and Privacy Badger are two products that include anti-trackers with their ad blockers, but Privacy Badger was the only company that could block tracking conducted by Facebook Like buttons.

rate.[192] Shortly after, Pew Research Center reported that 91% of Americans felt they had lost control over the way their personal data is collected and used.[193] A Forrester Research report showed that 19% of consumers had taken steps to activate the Do Not Track feature in their browsers—even though Do Not Track had no teeth.[194] The marketing materials of AdBlock, the #1 ad blocking software on the market, touted "Privacy is Paramount."[195] However, publishers whose livelihoods depended on advertising started to panic at the prospect of mass consumer adoption of ad blockers. AdBlock, and another anti-tracking software company called Disconnect, joined hands with privacy advocacy group Electronic Frontier Foundation, in an attempt to broker an agreement with publishers—if publishers would only respect users' activation of Do Not Track, they would drop their fences and stop blocking their ads.[196]

The use of ad blocking software by consumers rose in tandem with the market's ability to extract the rent of commercial surveillance. A 2015 joint study between Adobe and PageFair showed that there were 198 million people actively blocking ads, with a U.S. year-over-year growth rate of 48%.[197] In August of 2015, Apple announced that its new mobile operating system, IOS 9, would permit developers to introduce apps that enabled content blocking into the app store. When IOS 9 released in September, the top app downloads were immediately for ad

---

[192] Google Trends, GOOGLE.COM (2013-2014), https://trends.google.com/trends/explore?date=all&q=adblock; *see generally* PageFair, *The Rise of Adblocking,* PAGEFAIR.COM (2014), https://downloads.pagefair.com/downloads/2016/05/The-Rise-of-Adblocking.pdf.

[193] *See* Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RES. CTR. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

[194] *Privacy Is Far From Dead: Introducing Contextual Privacy*, FORRESTER RESEARCH (Dec. 19, 2013), https://www.forrester.com/Privacy+Is+Far+From+Dead+Introducing+Contextual+Privacy/-/E-PRE6624.

[195] *See* ADBLOCK, www.adblock.com.

[196] Press Release, Electronic Frontier Found., Coalition Announces New 'Do Not Track' Standard for Web Browsing (Aug. 3, 2015), https://www.eff.org/press/releases/coalition-announces-new-do-not-track-standard-web-browsing

[197] PAGEFAIR, *The 2015 Ad Blocking Report*, PAGEFAIR.COM (Aug. 10, 2015), https://pagefair.com/blog/2015/ad-blocking-report/.

blockers.[198] By 2016, reports showed that one in five smartphone users—or 420 million people worldwide—were blocking ads when browsing on the mobile web.[199] By 2017, a report from the advertising research company eMarketer estimated that one-quarter of U.S. internet users were blocking ads one way or another.[200] In tandem, independent studies conducted by the Pew Research Center, and the Annenberg Center, continued to show that Americans were overwhelmingly opposed to being shown ads targeted to them based on information derived from surveillance.[201] Was this the largest boycott in human history?[202]

Facebook raced to engineer a way to circumvent users' installation of ad blockers. Initially, Facebook prevented its public-facing pages from loading on user devices that had ad blockers installed. If consumers landed on forbes.com and Forbes prevented its page from loading, consumers could switch to a Forbes competitor to read news. With Facebook, consumers did not have any alternative product they could switch to. Then, in August of 2016, Facebook announced it had found a way to circumvent ad blockers entirely.[203] Facebook "flipped a switch on its desktop website that essentially renders all ad blockers … useless."[204] This time,

---

[198] Sarah Perez, *A Day After iOS 9's Launch, Ad Blockers Top the App Store,* TECHCRUNCH.COM (Sept. 17, 2015), https://techcrunch.com/2015/09/17/a-day-after-ios-9s-launch-ad-blockers-top-the-app-store/.

[199] PAGEFAIR, *Mobile Adblocking Report,* PAGEFAIR.COM (2016), https://pagefair.com/blog/2016/mobile-adblocking-report/; and Mark Scott, *Rise of Ad Blocking Software Threatens Online Revenue*, N.Y. TIMES (May 30, 2016), https://www.nytimes.com/2016/05/31/business/international/smartphone-ad-blocking-software-mobile.html.

[200] *Facing Up to Ad Blocking: How Publishers, Advertisers and their Digital Media Partners are Responding*, EMARKETER.COM (June 21, 2017), https://www.emarketer.com/Report/Facing-Up-Ad-Blocking-How-Publishers-Advertisers-Their-Digital-Media-Partners-Responding/2002077.

[201] *See* Mary Madden & Lee Raine, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RES. CTR. (May 2, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ (study revealed that 93% of American adults believe that having control over who gets their information is important; 88% said it is important that they are not watched or eavesdropped on without their permission ; 84% of respondents wanted control over what online marketers knew about them); Joseph Turow, Michael Hennessy & Nora Draper, *The Tradeoff Fallacy*, NEW ANNENBERG SURVEY RESULTS (2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

[202] *Beyond Ad Blocking – The Biggest Boycott in Human History*, DOC SEARLS BLOG: BLOGS.HARVARD.EDU (Sept. 28, 2015), https://blogs.harvard.edu/doc/2015/09/28/beyond-ad-blocking-the-biggest-boycott-in-human-history/.

[203] Facebook only had to block ads on desktop, because Facebook had already found way to serve ads in mobile apps that could not be touched by ad blockers.

[204] Mike Isaac, *Facebook Blocks Ad Blockers, but It Strives to Make Ads More Relevant*, N.Y. TIMES (Aug. 9, 2016), https://www.nytimes.com/2016/08/10/technology/facebook-ad-blockers.html.

Rothenberg proclaimed, "Facebook should be applauded for its leadership on preserving a vibrant exchange with its users."[205] Here too, Facebook's dominance played a role in its ability to devise a method to circumvent blockers.[206] Before long, Wehner was sharing on earnings calls the ad revenue growth Facebook was able to sustain by evading ad blockers. For example, on Facebook's Q3 2016 earnings call, Wehner pointed out that half of the 18% year-over-year revenue growth in desktop ads was "largely due to our efforts on reducing the impact of ad blocking."[207] From Q3 2016 to the end of Q2 2017, Facebook was able to make $709 million dollars circumventing ad blockers.[208]

With rapid consumer adoption of ad blockers and Facebook's unique ability to force onto consumers the presence of behaviorally targeted ads, Facebook approached publishers with a proposition. Facebook offered publishers the ability to publish content not on their own websites, but inside the walls of the impenetrable Facebook, where Facebook could ensure the delivery of behaviorally targeted advertising that commanded higher rates in ad markets.[209] Despite normally being competitors in the ad market, participating publishers like The New York Times worked in tandem with Facebook to sell the advertising. If a participating publisher sells the advertising, it keeps 100% of the ad revenue.[210] If Facebook sells the advertising for The New York Times, Facebook retains a 30% cut. Facebook had the power to force invasive advertising on consumers through a capability that other publishers like The New York Times did not

---

[205] *See id.*

[206] *See* Casey Johnston, *Why Facebook is Really Blocking the Ad Blockers*, THE NEW YORKER (Aug. 12, 2016), https://www.newyorker.com/business/currency/why-facebook-is-really-blocking-the-ad-blockers.

[207] *Facebook Inc. Q3 2016 Earnings Conference Call*, NASDAQ.COM (Nov. 2, 2016), https://www.nasdaq.com/aspx/call-transcript.aspx?StoryId=4018524&Title=facebook-fb-q3-2016-results-earnings-call-transcript.

[208] Johnny Ryan, *Facebook's Hackproof Ads Turned its Adblocking Problem in to a $709 Million Revenue Stream*, PAGEFAIR.COM (Nov. 2, 2017), https://pagefair.com/blog/2017/facebook-adblock-audience/.

[209] This is Facebook's Instant Articles program. *See Instant Articles* (July 2018), https://instantarticles.fb.com/.

[210] Facebook does not receive zero consideration in return. Facebook can monitor and measure the behavior of readers of Instant Articles and monetize this data in various ways.

have.[211] Facebook could successfully fight against users' preference for privacy—users had to submit to the terms of trade imposed upon them by this century's new communications network.

III. INDIRECT EVIDENCE CONFIRMS FACEBOOK'S MONOPOLY POWER

Facebook entered a competitive social media market and disintermediated competition by offering superior consumer privacy protections. Subsequently, Facebook tried to undermine privacy to initiate consumer surveillance for the purpose of delivering more targeted advertising, but the competitive market would not allow it. Only after other social networks like MySpace and Orkut exited the market, and Facebook amassed over a billion users, was Facebook able to reverse course, and initiate consumer surveillance. The fact-pattern demonstrates an inelasticity of demand for Facebook's product, and in turn, constitutes a direct showing of monopoly power under Section 2 of the Sherman Act. Facebook's ability today to extract surveillance in its exchange with consumers merely reflects an ability to extract monopoly rents from consumers that contradicts their own welfare. A review of indirect, or circumstantial, evidence of market power—to which I now turn—further explains Facebook's exhibited monopoly power over product quality. Facebook controls over 80% of the social network market and Facebook's control is protected by strong entry barriers which dissuade new-entrants.

Evaluating a market's structure by estimating a particular firm's percentage share of a market can be a useful mechanism for predicting a firm's market power, but should not be necessary to prove Facebook's monopoly power.[212] The goal of antitrust law is to protect

---

[211] *See* Johnston, *supra* note 206.

[212] *See generally* AREEDA & HOVENKAMP, §652, *supra* note 26 (articulating that Section 2 of the Sherman Act prohibits monopoly, which primarily refers to monopoly conduct, not monopoly shares, and going so far as to say, "Nothing in the language of the Sherman Act limits its conception of monopoly to large market share.") Note that in *Amex,* the Supreme Court did recently state that defining the relevant market is necessary despite direct evidence in cases alleging improper vertical restraints. Ohio v. Am. Express Co., 138 S. Ct. 2274 (2018).

consumers from the harms associated with a lack of competition—namely, increased prices, decreased quality, lower output, and less innovation. Often, direct proof of a company's ability to act like a monopolist is not available. In the absence thereof, circumstantial evidence of the market's structure can indicate whether a particular firm has monopoly power. Under this market share-market definition approach to analyzing power, the exercise becomes one of calculating Facebook's share of the relevant market. If one shows that Facebook controls a large percentage of a market that is protected by entry barriers, then this assertion serves as a proxy for direct proof of Facebook's ability to set price or define quality at levels that deviate from the competitive norm.[213] In Facebook's case, direct evidence of monopoly power exists, and this fact should obviate the need for isolating Facebook's share of a relevant market. Nonetheless, some scholars have argued that framing a defendant's power in terms of market structure may still be necessary to satisfy Section 2 statutory requirements.[214] In this respect, pleading a dominant share of a relevant market may serve a purpose outside the scope of proving power.

Under the market share-market definition framework, the first step is to isolate the relevant market from which firm's market share is deduced. The relevant market is that in which "significant substitution in consumption" occurs,[215] and should only include other products that consumers can turn to if one firm increases price or decreases quality.[216] In Facebook's case, the appropriate contours of the relevant market should only include other social networks that consumes use interchangeably. The purpose of defining the relevant market is to identify the swath of other products that can restrain a company's ability to extract monopoly rents.

---

[213] AREEDA & HOVENKAMP, §652, *supra* note 26.

[214] *See generally* AREEDA & HOVENKAMP, §531, *supra* note 26 (also noting that identifying a market's structure and defendant's share may be useful to distinguish between monopoly rents extracted by a single monopolist versus coordinating oligopolists").

[215] *See generally* AREEDA & HOVENKAMP, §5.02 *supra* note 26; *see also* United States v. Grinnell Corp., 384 U. S. 563, 571 (a market is restricted to reasonably "interchangeable services").

[216] *See generally Grinnell Corp.*, 384 U. S. at 571.

Empirically, an earlier competitive social network market appeared to do just this.[217] Competition from Murdoch's MySpace or Google's Orkut restrained how boldly Facebook (and others) could deteriorate quality given a constant price in a way that competition from instant messaging or email services today do not. In other words, Facebook's ability to deteriorate quality below competitive levels only after the exit of other social networks lends credence to the position that the relevant market should be limited to social networks.

Furthermore, the relevant market should be constrained to social networks because social networking is a new, unique, form of communications, unrivaled in its ability to distribute and amplify a consumer's communication. Whereas the telephone in the 20th century unleashed a watershed of one-to-one voice communications, the social network has opened the floodgates on one-to-many communications, distributed instantly from one person to others in a person's "social graph."[218] From the consumer's perspective, Facebook is merely a tool for digital communications.[219] The Facebook social media network enables instant one-to-many communication via text, audio, image, or video, exponentially decreasing the consumer's transactional costs that are associated with such widely distributed communications. Initially, Facebook marketed its social media platform as "a social utility."[220] By simply hitting the singular "post" button, a mother might share wedding pictures with hundreds, if not thousands, of close and extended family members, long-lost college friends, and acquaintances worldwide.

---

[217] *See generally infra* Part II.

[218] The term "social graph", initially popularized by Facebook itself and first referred to at the 2007 Facebook F8 conference, refers to a person's web of connections, and is the underlying business asset that a social network uses to distribute one's communication to one's contacts. *Facebook Unveils Platform for Developers of Social Applications*, NEWSROOM.FACEBOOK.COM (May 24, 2007), https://newsroom.fb.com/news/2007/05/facebook-unveils-platform-for-developers-of-social-applications/.

[219] On recent advertisements (as seen on nytimes.com medium rectangle ads on June 30, 2018), for example, Facebook marketed itself as a tool to "connect with friends and family." Also consider generally the marketing language on Facebook's website. *Bringing the World Closer Together,* FACEBOOK.COM (July 20, 2018), https://www.facebook.com/pg/facebook/about/?ref=page_internal.

[220] *Facebook Homepage*, FACEBOOK.COM (Nov. 29, 2007), http://www.facebook.com/ [http://web.archive.org/web/20071129130140/http://www.facebook.com/].

In this nation's earlier historic antitrust action against AT&T in the telephone market, the court defined the relevant market simply as "telecommunications," because the public interest was so served since telecommunications had come to play a dominant role in "modern economic, social, and political life."[221] Social media has come to dominate the American way of life in much the same way that the telephone did for earlier generations. The fabric of American politics, the roll-out of new consumer products, and the dissemination of news all unfold on social media. The sitting U.S. President's preferred way of communicating directly with the American people is through Twitter, one of the handful of social networks remaining today.[222] Two-thirds of Americans now receive news via social networks, with the majority receiving news via Facebook.[223] In some countries, the sheer amount of time citizens spends on social networks has become a matter of public health concern. Earlier this year, to address the time spent on social media, and the potentially addictive nature of such platforms, France passed legislation banning cell phones entirely from school grounds.[224]

In the United States, and across the world, Facebook in particular dominates the social network market. In the U.S. alone, 210 million consumers have a Facebook account,[225] with roughly three-fourths of those consumers using the platform at least once per day.[226] To put this in perspective, it was not until some 100 years after the invention of the telephone that the

---

[221] United States v. American Tel. and Tel. Co., 552 F. Supp. 131, 165 (D.D.C. 1983).

[222] Tamara Keith, *Commander-In-Tweet: Trump's Social Media Use and Presidential Media Avoidance*, NPR.ORG (Nov. 18, 2016), https://www.npr.org/2016/11/18/502306687/commander-in-tweet-trumps-social-media-use-and-presidential-media-avoidance.

[223] Elisa Shearer and Jeffrey Gottfried, *News Use Across Social Media Platforms 2017*, PEW RES, CTR. (Sept. 7, 2017), http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/.

[224] Sam Schechner, *France Takes on Cellphone Addiction with Ban in Schools*, WALL STREET J. (Aug. 13, 2018), https://www.wsj.com/articles/france-takes-on-cellphone-addiction-with-a-ban-in-schools-1534152600.

[225] The Facebook ads interface claims to reach 210 million consumers in the U.S. ages 13 and over. *Facebook Ads*, FACEBOOK.COM (July 20, 2018), https://www.facebook.com/business/products/ads.

[226] *See Social Media Fact Sheet*, PEW RES. CTR. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/social-media/.

telephone rivaled Facebook's penetration into the lives of American households.[227] But Facebook does not only cut wide, it also cuts deep. Americans currently spend over 40 minutes per day on just Facebook, and over an hour per day on Facebook owned-and-operated platforms, like Instagram.[228] U.S. consumers spend approximately 150 million hours per day on Facebook.[229] Facebook's dominance also crosses international borders. Across the world, around one in every four humans has a Facebook account. This means that of the population that has access to the internet, nearly one in every two persons that could have a Facebook account does.[230]

Within the realm of social networks, only platforms that consumers use interchangeably, and that bear on Facebook's demand elasticity, should be considered part of the relevant market for antitrust analysis. Here, particularly problematic for Facebook is the fact that of the U.S. adult population that uses any form of social media, nearly 99% use Facebook.[231] Subsets of consumers use Facebook in addition to one or more additional social networking platforms. This fact alone suggests that consumers do not find other social networking platforms to be adequate substitutes. Perhaps this is why when Senator Lindsey Graham (R-SC) asked Zuckerberg to name a product consumers could use instead of Facebook, Zuckerberg was unable to.[232]

The fact that consumers find it indispensable to use Facebook simply reflects the fact that speech on Facebook is more powerful than other methods of personal speech. As the only social

---

[227] *U.S. Census Bureau, Statistical Abstract of the United States: 1999* 885 (1999), www2.census.gov/library/publications/1999/compendia/statab/119ed/tables/sec31.pdf.

[228] EMARKETER.COM, *supra* note 71.

[229] *Id*.

[230] BROADBAND COMMISSION FOR SUSTAINABLE DEVELOPMENT, *The State of Broadband 2017: Broadband Catalyzing Sustainable Development Report* (Sept. 2017), https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.18-2017-PDF-E.pdf (estimating around 48% of global population had access to the internet at the end of 2017).

[231] *See* PEW RES. CTR., *supra* note 226 (69% of U.S. adults use social media; 68% of U.S. adults use Facebook).

[232] Unable to name a direct competitor, Zuckerberg explained that Google, Apple, Amazon, Microsoft, Twitter and other services generally overlap with Facebook in different ways. *See Facebook Congressional Hearing Before the Committees on the Judiciary and Commerce, Science and Transportation*, 115th Cong. (April 2018). For transcript of hearing *see Transcript of Zuckerberg's Senate Hearing*, WASH. POST (April 10, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?noredirect=on&utm_term=.17ef62e494e8.

network with a user-base of over 2 billion, Facebook connects its users to the largest number of people, and can distribute their speech more broadly than users could otherwise. On a recent earnings call, Sheryl Sandberg, chief operating officer of Facebook, touted Facebook as the place to "reach everyone [in] almost every country in the world."[233] One may not always want to speak loudly, but when one does, or one is selling a product, selling oneself for political office, or distributing news, Facebook distribution becomes a necessity.

Only Facebook has a user-base of over 2 billion. Competitive social networks with much smaller user-bases cannot directly compete with the built-in utility of Facebook's product.[234] This explains why competitors instead narrowly focus on carving out a sub-niche in the social network market—short tweets, disappearing messages, a social network for professionals. For example, the second largest social network, Instagram, has 1 billion users globally, about 88 million in the U.S., and allows people to communicate almost entirely through visuals.[235] Facebook, however, owns Instagram. LinkedIn is in third place with about 500 million users, with 133 million in the U.S., but focuses specifically on being a "professional network," enabling digital communication for "economic opportunity."[236] SnapChat has 191 million daily-active users worldwide, with approximately 72 million in the U.S., but distinguishes itself with short, disappearing pictures or videos.[237] Consider Twitter—with some 336 million monthly-active

---

[233] Sheryl Sandberg, *Facebook Inc. Q4 2017 Earnings Conference Call*, NASDAQ.COM (Jan. 31, 2018), https://www.nasdaq.com/aspx/call-transcript.aspx?StoryId=4141984&Title=facebook-s-fb-ceo-mark-zuckerberg-on-q4-2017-results-earnings-call-transcript.

[234] Since social networks today are closed communications protocols, each platform's utility is a function of the number of users found on a particular platform.

[235] *See Facebook Q1 2018 Quarterly Earnings Report*, FACEBOOK INVESTOR RELATIONS (April 25, 2018), https://investor.snap.com/~/media/Files/S/Snap-IR/reports-and-presentations/1q-18-10q.pdf*; Number of Instagram users in the United States from 2015 to 2021*, STATISTA.COM (Aug. 2017), https://www.statista.com/statistics/293771/number-of-us-instagram-users/.

[236] *About LinkedIn*, LINKEDIN.COM (July 20, 2018), https://about.linkedin.com/.

[237] *See Snap Inc. Q1 2018 Quarterly Earnings Report,* SNAP INVESTOR RELATIONS (May 2, 2018), https://otp.tools.investis.com/clients/us/snap_inc/SEC/sec-show.aspx?Type=html&FilingId=12721842&Cik=0001564408 (reporting 191 monthly Daily Active Users (DAUs) and 81 million DAUs in North America). SnapChat does not provide a breakdown of U.S. only users. But

users, with 68 million in the U.S., which constrains user text communication to no more than 280 characters.[238] For antitrust purposes, competing social networks—Instagram, LinkedIn, SnapChat, and Twitter—are not adequate substitutes because their user-bases are much smaller, and they serve a more narrow purpose.[239]

With regards to instant messaging services such as WhatsApp and video sharing services such as YouTube, consumers use these services in inherently different ways than they use social media platforms. Thus, they too are not substitutes. Sandberg recently explained the difference between Facebook and instant messaging platforms Messenger and WhatsApp to investors: social networks such as Facebook are about one-to-many communications, Messenger and WhatsApp are mainly about one-to-one communications.[240] Even so, Facebook also owns Messenger and WhatsApp. In response to an abuse of power investigation by Germany's cartel office, Facebook complained that the office's report "paints an inaccurate picture" of dominance because the report did not include Twitter, SnapChat *and* YouTube.[241] But for the consumer, YouTube is more interchangeable with television or subscription-video on demand (Amazon, HBO, etc.) than it is with Facebook. In a reflection of this, YouTube markets itself to advertisers as a substitute for television network spend.[242]

Facebook's U.S. reach is about 90% of Facebook's North America reach (210 million in the U.S. vs. 23 million in Canada). Assuming that SnapChat's U.S.-North America ratio is similar, we can estimate that SnapChat's U.S. DAU number is approximately 72.3 million. Statistica estimates that SnapChat's reach in the U.S. is approximately 77 million (not a DAU number). *Number of Snapchat Users in the United States from 2015 to 2021 (in millions)*, STATISTA.COM (Feb. 2017), https://www.statista.com/statistics/558227/number-of-snapchat-users-usa/.

[238] *Twitter Q1 2018 Quarterly Report*, TWITTER INVESTOR RELATIONS (April 25, 2018), https://investor.twitterinc.com/results.cfm. For a break-down of U.S. monthly active users; *Q2 2017 Letter to Shareholders*, TWITTER.COM (July 27, 2017), http://files.shareholder.com/downloads/AMDA-2F526X/4882764939x0x951006/4D8EE364-9CC3-4386-A872-ACCD9C5034CF/Q217_Shareholder_Letter.pdf.

[239] 15 U.S.C. § 2 (2000).

[240] *See* Sandberg, *supra* note 233.

[241] *See* Sam Schechner, *Germany Says Facebook Abuses Market Dominance to Collect Data*, WALL STREET J. (Dec. 20, 2017), https://www.wsj.com/articles/facebook-abuses-its-dominance-to-harvest-your-data-says-german-antitrust-enforcer-1513680355?.

[242] YouTube's marketing literature for advertisers focuses on this comparison, advertising the fact that "In an average month, 18+ year-olds in the United States spend more time watching YouTube than any television

Facebook will not be successful in arguing that it is a two-sided platform and that the boundaries of the relevant market definition should account not only for Facebook's share of the social network consumer market, but also its share of the digital advertising market. According to the Supreme Court's opinion in *Amex*, defendant American Express, as a credit card company, operated a two-sided "transaction" platform, so plaintiffs needed to prove defendant's conduct was cumulatively anticompetitive in both markets.[243] The district court had erred in treating the credit-card market as two separate markets—one for merchants and one for cardholders—and then only evaluating the anticompetitive effects to the merchant side of the market.[244] The Court in *Amex*, however, pigeonholed its holding to two-sided "transaction" platforms, where a company merely facilitates a simultaneous transaction between two parties. A transaction platform displays strong bi-lateral indirect network effects between the two distinct markets in which a defendant operates. With American Express, this appears true: more Amex cardholders always increases the value proposition for Amex merchants; and, more Amex merchants always increases the value proposition for Amex cardholders. Because of this, the relevant market has to include both sides. The Court pointed out a type of two-sided platform that might fail this rule—companies that deliver content to consumers, but advertising to marketers. Newspapers, it explained, fail the strong indirect networks effects test: more consumers are always good for advertisers, but more advertisers are not always good for consumers.[245] Two-sided platforms that

network." *Case Study: The Evolution of Digital Video Viewership*, NIELSEN.COM (Sept. 25, 2015), http://www.nielsen.com//content/dam/corporate/us/en/reports-downloads/2015-reports/nielsen-google-case-study-sept-2015.pdf.

[243] Ohio v. Am. Express Co., 138 S. Ct. 2274 at 2280 (2018).

[244] *Id.*

[245] *See Am. Express Co.* at 2281-82 ("A market should be treated as one sided when the impacts of indirect network effects and relative pricing in that market are minor. … But in the newspaper-advertisement market, the indirect networks effects operate in only one direction; newspaper readers are largely indifferent to the amount of advertising that a newspaper contains. … Because of these weak indirect network effects, the market for newspaper advertising behaves much like a one-sided market and should be analyzed as such.) (citing Lapo Filistrucchi, Damien Geradin, Eric van Damme, & Pauline Affeldt, *Market Definition in Two-Sided Markets: Theory and Practice* 1, 5 (Tilburg L. Sch. Legal Studs. Res. Paper Ser. No. 09/2013), *available at*

serve consumers on one side, but advertisers on the other, exhibit weak indirect network effects and should therefore be evaluated as one-sided markets for antitrust purposes. The Court's earlier precedent in the antitrust case against the Times-Piccayune newspaper in New Orleans supports this view. In *Times-Piccayune*, the Court considered a challenge to a newspaper's advertising policy and held that the relevant market includes only the newspaper's market share in advertising, not its market share in consumer readership.[246]

Under the second step of the market share—market definition analysis, market share should be derived from Facebook's quantitative share of consumer time on social networks. Share of consumer time on social networks is the relevant measure of market share for two distinct reasons. First, Facebook does not charge users a fee, some competitors do, and a measure must be able to account for all competitors in the market.[247] More importantly, consumer time is the barometer which Facebook and other social networks use in the market—on the ground so to speak—to signal their relative dominance. On this point, the Supreme Court has indicated that one should calculate market share in the way that market participants think and talk about it. For example, in *Ohio v. American Express Co.*, the Supreme Court calculated the market share of credit card companies based on transaction volume, not transaction revenues—to reflect how

---

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2240850 and Times-Picayune Publishing Co. v. United States, 345 U. S. 594, 610 (1953)).

[246] *Times-Picayune Publishing Co.*, 345 U. S. at 610.

[247] While Instagram, SnapChat and Twitter do not charge users a price, competitor Vero Social, which surged to the #1 downloaded app on the Apple app store early 2017 following news of Facebook privacy breaches, offers an ad-free, subscription model. *See* Todd Spangler, *Vero Hits No. 1 on Apple's App Store, But Can Subscription Social Network Sustain the Hype?* VARIETY (Feb. 27, 2018), https://variety.com/2018/digital/news/vero-social-app-store-ad-free-social-hype-1202711654/. Additionally, Zuckerberg and Sandberg have made comments to U.S. Congress and NBC news respectively that suggest Facebook itself may introduce an ad-free, subscription version of Facebook. *See generally,* Callum Borchers, *Would You Pay $18.75 for Ad-Free Facebook?* WASH. POST (April 14, 2018), https://www.washingtonpost.com/news/the-fix/wp/2018/04/14/would-you-pay-18-75-for-ad-free-facebook/?utm_term=.833d67a1fefc.

market participants themselves signal their relative dominance.[248] Social networks, including Facebook, Instagram, Twitter, and SnapChat speak of their relative strength in the social network market by referring specifically to the number of users and the number of minutes spent by users on their platform.[249]

However, even if one were to consider Instagram, Twitter, and SnapChat as part of the relevant market for antitrust analysis, Facebook *still* dominates market share. Including time spent on these other platforms, approximately 83% of the consumers' time goes to Facebook and Instagram.[250] Consumers spend about 66% of time across all on just Facebook, 17.5% of time on Instagram, 16% on SnapChat, and 0.5% of time on Twitter. Anecdotally, Americans spend 19% of time spent across all mobile applications on just the Facebook mobile app.[251]

Facebook's control of over 80% of consumer time reflects Facebook's monopolistic power in the social network market. While there is no bright-line rule regarding market shares, courts have assumed monopoly power when market shares exceed over 70-plus percent.[252] For example, before the dissolution of AT&T for monopoly power in the interexchange market, AT&T's share of interexchange revenue was about 77%.[253] Standard Oil, found to have illegally monopolized the oil market, controlled about 90% of refinery output.[254]

---

[248] Ohio v. Am. Express Co., 138 S. Ct. 2274 (2018) (American Express was found to only control 26.4% of the credit card market because it controlled 26.4% of transaction volume).

[249] Consider the fact that social network advertising media kits focuses on the number of users and number of minutes spent on their social networks.

[250] I multiplied most-recent U.S. user numbers of each platform (Facebook 210 million, Instagram 88 million, SnapChat 77 million, Twitter 68 million) by the number of average minutes spent by users per day on each (Facebook 41 minutes, Instagram 26, SnapChat 27, Twitter 1) to find a total market size of 13,045,000,000 minutes per month. *See* EMARKETER.COM, *supra* note 71.

[251] Simon Khalaf, *U.S. Consumers Time-Spent on Mobile Crosses 5 Hours a Day*, FLURRY ANALYTICS BLOG (March 2, 2017), http://flurrymobile.tumblr.com/post/157921590345/us-consumers-time-spent-on-mobile-crosses-5.

[252] *See* United States v. Grinnell Corp., 384 U. S. 563, 571 (1966) (market share exceeding 87% is predominant); Eastman Kodak Co. v. Image Technical Servs., Inc., 504 U.S. 451, 481 (1992) (market share exceeding 80%); United States v. E. I. du Pont de Nemours & Co., 351 U.S. 379, at 391 (1956) (market share exceeding 75%).

[253] United States v. Am. Tel. and Tel. Co., 552 F. Supp. 131 (D.D.C. 1983).

[254] Standard Oil Co. of New Jersey v. United States, 221 U.S. 1 (1911).

Notwithstanding Facebook's dominant share of the relevant market, market share analysis also considers whether firms are protected by barriers to entry.[255] Without entry barriers, new entrants have the opportunity to quickly disintermediate even the most dominant firms. The mere threat of entry can prevent monopolists from being able to profitably extract monopoly rents from consumers. But, there are entry barriers associated with Facebook's *closed* communications protocol and over 2 billion users. When a communications network is closed, a user can only communicate with another user of the same network. This creates a powerful phenomenon known as direct network effects.[256] Just as the utility of owning a phone in the late 19th century grew as phones became more accessible, so does the utility of a closed social network depend on how many other people use it. A new market entrant cannot easily get users to switch to a platform with less users. Additionally, the lack of perfect substitutes for Facebook has allowed the company to have proprietary control over one's social graph. Facebook's users are often connected exclusively through Facebook's network, may lose cell phone numbers for older contacts, and Facebook becomes the primary method for users to remain in contact with one another. Because the communications protocol is closed, and Facebook controls one's social graph, consumers face high switching costs and competitors face a significant barrier to entering the market.

---

[255] United States v. Microsoft Corp., 253 F.3d 34 (D.C. Cir. 2001).

[256] A product has direct network effects if one's use of a product increases the product's utility for others. For example, in a market with only two competing social networks, assuming constant price and quality, the network with the larger user-base has greater value because it allows new users to communicate with more people. Other businesses with strong network effects include those of Uber, Wikipedia, and Airbnb. In such markets, the company that achieves early gains begins immediately to benefit from the superiority of one's product due to network effects. The concept of network effects was first identified in the context of the long-distance telephony market in the 1970s. *See* Jeffrey Rohlfs, *A Theory of Interdependent Demand For A Communications Service*, THE BELL J. OF ECON. AND MANAGEMENT SCI, 16–37 (1974). Subsequent papers on this topic include W. BRIAN ARTHUR, ON COMPETING TECHNOLOGIES AND HISTORICAL SMALL EVENTS: THE DYNAMICS OF CHOICE UNDER INCREASING RETURNS (1983); Joseph Farrell & Garth Saloner, *Standardization, Compatibility, and Innovation*, THE RAND J. OF ECON. 70–83 (1985); Michael L Katz & Carl Shapiro, *Network Externalities, Competition, and Compatibility*, 75 THE AM. ECO. REV. 424 (1985). During the first dot-com rush, venture capitalists and entrepreneurs in Silicon Valley were keenly in-tune and in-favor of investing in companies that benefited from direct network effects, or "first-mover advantage." *See generally* Eric Ransdell, *Network Effects*, FASTCOMPANY.COM (Aug. 31, 1999), https://www.fastcompany.com/37621/network-effects.

IV. FACEBOOK'S PATTERN OF CONDUCT RAISES CONCERNS ABOUT ILLEGAL MONOPOLIZATION

A remaining question is whether Facebook's pattern of behavior reaches the level of anticompetitive conduct with which antitrust law concerns itself. Parts I and II of this Paper traced the particular history of Facebook's conduct with respect to the quality of its product. The qualitative aspects of its product, particularly the level of privacy, is not abstract—Facebook's product is free, privacy was a critical form of competition in a functioning market, citizens favor no surveillance, and extracted surveillance is strongly tied to current Facebook revenues and profits. Part II argued that Facebook's broad-scale surveillance of American consumers today reflects monopoly rents, a conclusion also supported by indirect evidence of Facebook's monopoly power considered in Part III. Part IV now contends that Facebook's conduct, taken collectively, raises serious issues of anticompetitive practices. Facebook's conduct engendered trust in consumers, but the record suggests that Facebook's commitment to user privacy was disingenuous. Facebook's course of misleading conduct resulted in precisely the type of harm that antitrust law concerns itself with—the exit of rivals and the subsequent extraction of monopoly rents in contravention to consumer welfare.

A. Heightened Scrutiny in Markets with Direct Network Effects

Though Facebook may be a monopoly, antitrust law, and the Sherman Act specifically, only condemns monopolies that acquired their power by engaging in anticompetitive conduct.[257]

[257] 15 U.S.C. § 2 (2000).

The classic definition of anticompetitive conduct is "the willful acquisition or maintenance of [monopoly] power as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident."[258] In other words, anticompetitive conduct falls outside the bounds of "competition on the merits."[259] It includes behavior that can be described as "predatory," "exclusionary," "unethical," or "deceptive."[260] Though scholars debate when deception is actionable under antitrust laws, as opposed to merely under consumer protection statutes, even the leading antitrust treatise concedes that deception falls into the category of prohibited, anticompetitive, conduct, when deception has made "a durable contribution to the defendant's market power."[261]

Courts have a broad mandate to capture and regulate a range of conduct that harms the competitive process and is likely to or does result in harm to consumers.[262] The breadth and flexibility that courts have reflects the fact that "monopolization [conduct] has tended to be

---

[258] In *United States v. Grinnell Corp.*, the Court articulated what remains the two-part test for a Section 2 violation: "(1) the possession of monopoly power in the relevant market and (2) the willful acquisition or maintenance of that power as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident." 384 U. S. 563, 571.

[259] *Microsoft Corp.*, 253 F.3d (finding Microsoft conduct outside the scope of "competition on the merits" to be anticompetitive).

[260] *See* Aspen Skiing Co. v. Aspen Highlands Skiing Corp., 472 U.S. 585, 605 (1985); Allied Tube & Conduit Corp. v. Indian Head, Inc., 486 U.S. 492, 500 (1988) (stating that "unethical and deceptive practices can constitute abuses of administrative or judicial processes that may result in antitrust violations"); Spectrum Sports, Inc. v. McQuillan, 506 U.S. 447, 458 (1993) (defining anticompetitive conduct generally as "conduct which unfairly tends to destroy competition itself"). *See also* AREEDA & HOVENKAMP, *supra* note 26; ROBERT H. BORK, THE ANTITRUST PARADOX 138 (1978) ("If a firm has been 'attempting to exclude rivals on some basis other than efficiency,' it is fair to characterize its behavior as predatory."). For an overview of how federal agencies and courts evaluate a monopolist's deception, see Maurice E. Stucke, *How Do (and Should Competition Authorities Treat a Dominant Firm's Deception*, 63 SMU L. REV. 1069 (2010). For a conversation on deception specifically, see Kevin S. Marshall, *Product Disparagement Under the Sherman Act, Its Nurturing and Injurious Effects to Competition, and the tension Between Jurisprudential Economics and Microeconomics*, 46 SANTA CLARA L. REV. 231, 244 (2006) (explaining that deception can "create entry barriers, lead to capricious market exit, create artificial market equilibrium, or even lead to oligopolies and monopolies.").

[261] AREEDA & HOVENKAMP, §782, supra note 26 (additionally, scholars point out that in situations where deception by a monopolist is at issue, the concern should be deception of consumers).

[262] *See* Herbert Hovenkamp, *The Monopolization Offense*, 61 OHIO ST. L. J. 1035 (2000), https://kb.osu.edu/bitstream/handle/1811/70413/OSLJ_V61N3_1035.pdf;sequence=1.

nonrepetitive and specific to industry."[263] Standard Oil's strategies in the oil market differed from American Tobacco's strategies in the tobacco market, AT&T's approaches in the telephony market, or Microsoft's tactics in the operating system market.

Moreover, anticompetitive conduct in the acquisition of monopoly power is of heightened concern in markets exhibiting direct network effects. In such markets, meaningful competition only exists at the early stages. At the beginning competition is fierce—each company vies to edge-out competitors to "tip" the market in its favor.[264] If a company can achieve early adoption with consumers, it can thereafter benefit not only from its product's price or quality, but also simply from its user-base—a feature that strongly influences consumer choice. Because of these market dynamics, the Court of Appeals for the D.C. Circuit in the monopolization case against Microsoft explained that competition in networked industries is often "for the field" rather than "within the field."[265] Misleading, deceptive, or otherwise unethical conduct at the early stages can induce market participants to choose the firm that they think increases their welfare, but the very act of mistaken choice can lock in the market to their detriment. Carl Shapiro, then deputy assistant attorney general for economics in the Antitrust Division of the Department of Justice, addressed the need for heightened concern: "Even more so than in other areas, antitrust policy in network industries must pay careful attention to firms' business strategies, the motives behind

---

[263] *Id.* at 1037.

[264] Theoretical economist W. Brian Arthur has published several papers discussing the unique nature of in markets characterized by network effects. His seminal paper is ON COMPETING TECHNOLOGIES AND HISTORICAL SMALL EVENTS: THE DYNAMICS OF CHOICE UNDER INCREASING RETURNS, *supra* note 256. *See also* MALCOLM GLADWELL, THE TIPPING POINT: HOW LITTLE THINGS CAN MAKE A BIG DIFFERENCE (2006); William J. Kolasky, Jr. & William F. Adkinson, Jr., *Single Firm Conduct: Who's Big? What's Bad?* Presentation Before the A.B.A. Sec. of Antitrust L. 30 (Apr. 15, 1999) (on file with author) (stating that "if the ultimate market outcome is likely to be a monopoly of the surviving firm, with the opportunity to earn substantial rents, competition among firms to be the survivor will be intense.").

[265] United States v. Microsoft Corp., 253 F.3d 34, 50 (D.C. Cir. 2001) (citing Harold Demsetz, *Why Regulate Utilities?*, 11 J. OF L. & ECON. 55, 57 (1968)).

these strategies, and their likely effects…."[266] In that vein, even Robert Bork, leader of Chicago-school antitrust jurisprudence, may have agreed when he advised that one must pay attention to the "route by which [monopoly] was gained."[267]

Such was the focus of the Court's analysis of Microsoft's misleading behavior in the operating system market.[268] Microsoft had made false public representations about its own products which induced developers to develop applications compatible with Microsoft's operating system. While Microsoft represented that applications developers wrote would be cross-compatible with Sun, developers ended up writing applications that were only compatible with the Windows operating system. Microsoft's false statements induced developers to choose Microsoft to their detriment. Since the operating system market exhibits direct network effects, misleading behavior to induce choice is anticompetitive. This was anticompetitive conduct that supported the finding that Microsoft had illegally monopolized the operating system market.

B. Pattern of False Statements, Misleading & Deceptive Conduct

A substantive issue is whether Facebook's pattern of conduct was anticompetitive and provides a basis for a claim of illegal acquisition of monopoly power. To begin, Facebook entered the market with superior privacy protections making promises to not violate user privacy which induced early consumer reliance.[269] For several years, in a hotly competitive market, Facebook did not merely change its privacy representations, it continued to perpetuate them. But

---

[266] Shapiro, *supra* note 26 (explaining that "the very nature of the 'positive feedback' cycle means that monopolization may be accomplished swiftly. And, once achieved, the network effects that helped create dominance may make it more difficult for new entrants to dislodge the market leader than in other industries lacking network characteristics.").

[267] BORK, *supra* note 260 at 164.

[268] *Microsoft Corp.*, 253 F.3d at 76-77.

[269] FACEBOOK PRIVACY POLICY (2004), *supra* note 42.

while perpetuating the belief that Facebook did not track consumers using third-party code, Facebook was caught doing precisely that on multiple occasions.[270] The investigative efforts of multiple independent researchers unveiled that the claims Facebook was making to consumers via Facebook's own policies and the public comments of Facebook executives were false.[271] Facebook itself even conceded their falsity.[272]

Facebook then deflected consumer concern over the discovered hidden activity and false statements with words and actions that implied the sincerity of Facebook's commitment to user privacy. For example, when Facebook's hidden activity and false statements with Beacon were exposed, Facebook retreated and Zuckerberg called Beacon a "mistake."[273] Later, when Facebook's hidden activity and false statements with social plugins were exposed, Facebook claimed that discovered tracking was due to inadvertent software "bugs" or that the tracking was innocuous because it was for users' own "safety and protection."[274] At the time, the chief technology officer of Facebook assured, "[social plugins are] not intended for tracking," rather user data collected was used "to protect the site from cyber-attacks by people who try to break in to users' accounts."[275] An evidentiary question is whether this activity was in fact inadvertent and for users' safety and protection or not. An investigation into the credibility of Facebook's alleged reasoning by the German Data Protection Authorities in Schleswig-Holstein found it without merit.[276] If Facebook's reasoning was factually inaccurate, as the GDPA investigation suggested, then Facebook's behavior was deceptive.

---

[270] *See infra* Section I.B & I.C.

[271] *Id.*

[272] *See* Perez, *supra* note 90.

[273] *See* Zuckerberg, *supra* note 109.

[274] *See infra* Section I.B.

[275] *See* Efrati, *supra* note 133.

[276] KIEL, UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN (ULD): DATENSCHUTZRECHTLICHE BEWERTUNG DER REICHWEITENANALYSE DURCH FACEBOOK (2011), https://www.datenschutzzentrum.de/uploads/facebook/20110930-facebook-verantwortlichkeit.pdf (conclusion based

In addition to perpetuating factual inaccuracies, Facebook deceived users by omitting salient facts.[277] Notably absent from public commentary was the fact that Facebook was thinking about, or planning on, using social plugins for surveillance. In 2011, Facebook had filed a patent for engaging in this type of behavior that was of public concern.[278] The Federal Trade Commission's case for illegal monopolization against Intel centered on Intel's misleading behavior.[279] For example, the FTC's complaint alleged that Intel had engaged in deceptive acts by failing to disclose material information about the effects of its products. When Facebook's surveillance conduct with plugins was discovered, Facebook provided affirmative, innocuous, and possibly false reasoning for its actions while omitting information related to Facebook's internal dialogue about using plugins to conduct surveillance. Facebook likely deceived market participants.

In retrospect, Facebook's widely-covered public announcement of a user referendum process for future privacy changes in the competitive market of 2009 may also raise issues of anticompetitive behavior. Facebook's poor notice to consumers in 2011—when it proposed and passed an abolishment of user voting—suggests that Facebook's commitment to the user referendum was less than genuine. Consumers ultimately felt cheated that Facebook did not notify them of an opportunity to vote.[280] Indeed, internal comments by employees suggest that Facebook made public representations about valuing privacy when in fact internally Facebook's

---

on finding that Facebook internal technical documentation for consumer protection and prevention did not depend on the use or reference of user cookies). S*ee also* Arnold Roosendaal, *Privacy and Identity § Massive Data Collection By Mistake*, in PRIVACY AND IDENTITY MANAGEMENT FOR LIFE 274-282 (Camenisch et al. ed., 2012).

[277] Deception can occur when one fails to disclose a fact that wrongfully causes a false belief in another. *See generally* Gregory M. Klass, *The Law of Deception: A Research Agenda*, 89 U. COLORADO. L. REV. 707 (forthcoming 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3156625.

[278] *See* U.S. Patent, *supra* note 147.

[279] Complaint in the Matter of Intel Corp., Case 0610247 (F.T.C. 2009) (No. 9341); Decision and Order in the Matter of Intel Corp. No. 9341 (F.T.C. 2009).

[280] *See supra* notes 150-153 and accompanying text.

culture and practices were not concerned with user privacy. Facebook employees themselves sometimes parodied this disingenuous public-private disconnect.[281]

C. Wider Pattern of False Statements and Misleading Conduct

Importantly, Facebook's wider history may point to a larger pattern of misleading conduct within the company. In 2011, Facebook settled charges with the Federal Trade Commission alleging a range of false and misleading material statements made to consumers related to user privacy—all of which fell outside of the scope of Facebook's conduct that is the focus of this Paper.[282] For instance, the FTC complaint alleged that while Facebook's privacy controls allowed users to restrict their information to "only friends," Facebook was actually overriding user choice and sharing users' information with third-parties. More recently, Facebook has come under congressional scrutiny for deceiving consumers by knowing but not disclosing to users that their data was misappropriated by political consulting firm Cambridge Analytica. When asked by Senator Kamala Harris (D-CA) if Facebook made an explicit decision to not inform users, Zuckerberg answered "yes," and called it another "mistake."[283] The wider record of deceptive conduct with respect to user privacy may also be relevant to a larger case of unlawful acquisition (and even perpetuation) of monopoly power.

Moreover, buyers of Facebook advertising would be keenly familiar with other "mistakes" and alleged "bugs" that Facebook claimed inadvertently caused a string of inflations

---

[281] *See* Tsotsis, *supra* note 154; *see* Martinez, *supra* note 154.

[282] *Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy*, FTC.GOV (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep; Complaint for violation of the Federal Trade Commission Act in the matter of Facebook Inc., No. 0923184 (F.T.C. Dec. 5, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf.

[283] *Mark Zuckerberg Testimony: Senators Question Facebook's Commitment to Privacy*, N.Y. TIMES (April 10. 2018), https://www.nytimes.com/2018/04/10/us/politics/mark-zuckerberg-testimony.html.

in ad metrics, which financially benefited Facebook to the detriment of buyers. A full review of Facebook's conduct (and pricing power) on the advertising side of the market is outside the scope of this Paper. However, I review here two incidents on the advertising side that suggest a larger pattern of willful disregard for truth. Aside from lending credence to a pattern and practice of false statements and misleading conduct, Facebook's behavior generally reflects pricing power on the advertising side of the market.

For example, in September of 2017, media buyers became aware that Facebook materials claimed to reach more people in the U.S. than Census data shows even existed.[284] The false representations are made in Facebook's self-serve interface that businesses use to evaluate and purchase Facebook advertising and are the subject of a recently filed class action complaint.[285]

To give another example, Facebook recently admitted to a succession of false statements related to ad metrics which induced marketers to purchase Facebook ads. For many years, Facebook did not allow ad buyers to audit and verify Facebook representations directly correlated to Facebook ad billing—despite audit rights being standard practice in the industry.[286] Facebook advertising is subject to elevated risks of fraud. Unlike print advertising, digital advertising is shown only briefly to a user and poof disappears forever. In other words, without audit rights, digital media buyers suffer from the risk of sellers charging them for goods not delivered *at all*. Facebook has long been a hold-out in permitting buyers to audit Facebook

---

[284] The initial discrepancy was caught and pointed out in a note to investors by respected industry analyst Brian Wieser. *See supra* note 15; *see also* Allison Schiff, *Facebook Data May Be at Odds with Census Data, But Advertisers Won't Stop Spending*, ADEXCHANGER.COM (Sept. 6, 2017), https://adexchanger.com/platforms/facebook-data-may-odds-census-data-advertisers-wont-stop-spending/

[285] Complaint, *Danielle A. Singer v. Facebook Inc.*, Case 4:18-cv-04978-KAW, (USDC N.D. Cal., Aug. 15, 2018).

[286] A refusal to submit to audits is a demonstration of pricing power on the advertising side of the market. Facebook's conduct reminds us of Yellow Pages' behavior in the print advertising market. Yellow Pages was also a hold-out, not allowing buyers to audit Yellow Pages' distribution figures. Yellow Pages, of course, was also a monopoly. ASS'N OF NAT'L ADVERTISERS TELEPHONE DIRECTORY COMMITTEE AND AM. ASS'N OF ADVERTISING AGENCIES DIRECTORY ADVERTISING COMMITTEE, THE NEED FOR YELLOW PAGES THIRD-PARTY CIRCULATION AUDITING (2005), *available at* http://www.ana.net/getfile/67.

deliverables. The head of digital marketing at Wendy's, who is currently the chief marketing officer of Papa John's, once explained, "[w]hat frustrates us when we run a campaign [on Facebook] is that there's almost no acknowledgement that the campaign even existed in the first place."[287]

After mounting industry pressure and calls of fraud, Facebook capitulated and announced in the fall of 2015 that it would allow third-parties to audit select metrics.[288] With the impending release of the first audited metrics, Facebook came forward with disclosures of discovered "bugs" that had caused it to inadvertently inflate ad metrics for multiple years.[289] In September 2016, Facebook revealed that it had overestimated customers' video ad view-times for the last two years. Facebook sent a letter to Publicis, one of the largest ad agencies in the world with a market cap of over $12 billion, estimating that it had overstated view times by 60-80%. Publicis had spent $77 million on Facebook ads the prior year. Publicis, in turn, sent a note out to clients: "This once again illuminates the absolute need to have ... verification on Facebook's platform. Two years of reporting inflated performance numbers is unacceptable."[290]

---

[287] Allison Schiff, *Facebook: Counting Viewed Impressions is a 'No Brainer'*, ADEXCHANGER.COM (Feb. 18, 2015), https://adexchanger.com/online-advertising/facebook-counting-viewed-impressions-is-a-no-brainer/#comment-911780. *See also* Jessica Davies, *'Facebook doesn't operate with real-world metrics': GroupM talks tough on Facebook*, DIGIDAY.COM (Sept. 21, 2018), https://digiday.com/media/facebook-doesnt-operate-real-world-metrics-group-m-talks-tough-facebook/ (where an executive at WPP, Facebook's largest single client, states: "We are still not able to verify delivery of our clients' advertising via Facebook … They control the delivery of consumption data back to us. We also have major issues with the quality of the environment our ads are delivering in, especially when it comes to Facebook. Also, completion rates on Facebook are appallingly low.").

[288] Tim Peterson, *Facebook to Sell 100% In-view Ads, Let Brands Fact-check Video Ad Views*, ADAGE.COM (Sept. 17, 2015), http://adage.com/article/digital/facebook-adds-ad-viewability-verification-options/300409/.

[289] Lindsay Stein, *ANA Calls Facebook Metrics to be Audited and Accredited*, ADAGE.COM (Sept. 29, 2016), http://adage.com/article/cmo-strategy/ana-calls-facebook-metrics-audited-accredited/306096/?CSAuthResp=1515363470777:0:2255529:0:24:success:5A7B779E9C26F932284F303D3DF677EA; Suzanne Vranica & Jack Marshall, *Facebook Overestimated Key Video Metric for Two Years*, WALL STREET J. (Sept. 22, 2016), https://www.wsj.com/articles/facebook-overestimated-key-video-metric-for-two-years-1474586951.

[290] Vranica & Marshall, *supra* note 289.

Between November and December of 2016, Facebook disclosed additional measurement misreporting.[291] Facebook had been inflating the number organic visits to brand posts, over-reporting by 7-8% the average length of time people spent reading Instant Articles, over-stating video ad completion rates, over-reporting the number of clicks it had reported it sent to advertiser websites, over-reporting the number of Likes for live videos, and inflating the number of times people shared links of posts on Facebook. Advertisers used these metrics to ask and inform imperative questions: is this advertising campaign working? and should I spend more or less money in the future with Facebook?

The Association of National Advertisers (ANA) subsequently publicly called for an in-depth general audit, as they once did with the Yellow Pages—which is still pending.[292] P&G's chief brand officer, Marc Pritchard, has warned that systemic fraud in ad markets may explain the U.S. economy's anemic growth.[293] Pritchard has publicly pressured Facebook to submit to transparency, and likened Facebook's self-policing to letting a "fox guard the hen house." Advertising agencies, the middlemen in ad buys, were and continue to be in an awkward position, having been entrusted to spend their brands' money wisely. The chief operating officer of GroupM, the media buying arm of ad agency behemoth WPP, lamented at an industry

---

[291] James Hercher, *Facebook Jumps Out of the Frying Pan and Into Fire with More Measurement Errors*, ADEXCHANGER.COM (Nov. 16, 2016), https://adexchanger.com/platforms/facebook-jumps-frying-pan-fire-metric-errors/; Garett Sloane, *Now Facebook Says it Gave Some Publishers Bad Traffic Numbers on Instant Articles*, ADAGE.COM (Dec. 16, 2016), http://adage.com/article/digital/facebook-gave-publishers-bad-traffic-numbers/307192/.

[292] Jack Marshall, *ANA Pushes Facebook for Greater Measurement Transparency*, WALL STREET J., (Sept. 30, 2016), https://www.wsj.com/articles/ana-pushes-facebook-for-greater-measurement-transparency-1475186796; Allison Schiff, *Facebook Gets Its First MRC Accreditation, But There's Still More To Go*, ADEXCHANGER.COM (April 5, 2018), https://adexchanger.com/platforms/facebook-gets-its-first-mrc-accreditation-but-theres-still-more-to-go/.

[293] Jack Neff, *P&G Tells Digital to Clean Up, Lays Down New Rules for Agencies and Ad Tech to Get Paid*, ADAGE.COM (Jan. 29, 2017), http://adage.com/article/media/p-g-s-pritchard-calls-digital-grow-up-new-rules/307742/; Marc Pritchard, Chief Brand Officer, Speech given at Interactive Advertising Bureau's Annual Leadership Meeting (Jan. 29, 2017), available at https://www.youtube.com/watch?v=NEUCOsphoI0.

conference that Facebook is one of the only ones that can measure themselves, and it is a result of "Facebook's market dominance."[294]

D. Antitrust Harm: Monopoly Rents & Allocative Inefficiency

Ultimately, Facebook's course of conduct misled consumers and resulted precisely in the type of harm with which antitrust law concern itself.[295] Facebook today is a monopoly that has the power to extract monopoly rents from consumers, as detailed in Section II-C. Facebook's collective conduct—specifically, false statements, misleading statements, and omissions—reviewed in Part I and Part II, contributed to this ultimate destination. The harm is not speculative, it is complete. This new age's communications utility extracts the cost of widespread digital surveillance despite users' preference to the contrary.

The tendency is to think that Facebook's free service reflects consumer surplus, yet nearly every advertising market in the U.S. is in decline as American consumers indicate a preference for ad-free communications and media. In the world of television and video, consumers have flocked from ad-supported TV to ad-free, over-the-top competitors. In that world, Netflix, Amazon, and HBO, all paid, ad-free platforms, are bathing in a watershed moment of creativity and high consumer satisfaction.[296] With radio, terrestrial loses ground to digital alternatives that offer subscriptions to ad-free music streaming. While digital music

---

[294] Allison Schiff, *Facebook And GroupM Tussle on Third-Party Viewability Verification*, ADEXCHANGER.COM (June 3, 2015), https://adexchanger.com/online-advertising/facebook-and-groupm-tussle-on-third-party-viewability-verification/

[295] Consumers have standing to sue for quality reductions. *See* AREEDA & HOVENKAMP, ¶¶ 345, 502, *supra* note 26 (stating that "clearly a consumer has standing to sue a cartel that reduces quality of the product that the consumer purchased"). Facebook's 2014 decisions to initiate consumer surveillance are also anticompetitive in the sense that they make it more difficult for new entrants like SnapChat to compete with Facebook on the advertising side of the market.

[296] The American Customer Satisfaction Index (ACSI), an annual survey of consumer attitudes to services including pay TV, video streaming, ISPs and fixed and wireless phone.

platforms can be ad-supported or ad-free, the paid but ad-free models currently drive the largest share of growth in the industry.[297] In the digital advertising market, most sellers of digital advertising struggle to obtain incremental, year-over-year revenue growth. In the midst of a booming economic cycle in 2017, *The Guardian*, Britain's nearly 200-year-old daily newspaper, started to ask readers for donations after digital ad revenues fell.[298] BuzzFeed followed suit.[299] However, the market is growing. The U.S. internet advertising market grew 21.8% in 2016 and 21% in 2017. Facebook and Google accounted for over 99% and over 90% of that growth in 2016 and 2017, respectively.[300] Consumer studies show that consumers today are averse to advertising.[301]Against this backdrop, Facebook's free but ad-supported communications service, built upon a massive commercial surveillance apparatus, may indeed reflect one great allocative inefficiency in markets.

CONCLUSION

"Monopoly in trade or in any line of business in this country is odious to our form of government .... its tendency is repugnant to the instincts of a free people."

—Chief Justice Sherwood of the Supreme Court of Michigan.[302]

---

[297] *See* MORGAN STANLEY, LEADERS CONSOLIDATING: OUR 4TH ANNUAL MUSIC & RADIO SURVEY 8 (Dec. 17, 2017), https://fa.morganstanley.com/balog/mediahandler/media/111221/Morgan%20Stanley%204th%20Annual%20Music%20and%20Radio%20Survey.pdf.

[298] David Bond, *Guardian Relies on Readers' Support to Stave Off Crisis*, FINANCIAL TIMES (May 13, 2017), https://www.ft.com/content/9044ff9a-358b-11e7-99bd-13beb0903fa3.

[299] Benjamin Mullin, *BuzzFeed News Asks Readers to Chip in With Donations*, WALL STREET J. (Aug. 27, 2018), https://www.wsj.com/articles/buzzfeed-news-asks-readers-to-chip-in-with-donations-1535395575

[300] Sarah Sluis, *Digital Ad Market Soars To $88 Billion, Facebook And Google Contribute 90% Of Growth*, ADEXCHANGER.COM (May 10, 2018), https://adexchanger.com/online-advertising/digital-ad-market-soars-to-88-billion-facebook-and-google-contribute-90-of-growth/.

[301] MILLWARD BROWN, *AdReaction Gen X, Y and Z Executive Summary*, http://www.millwardbrown.com/adreaction/genxyz/global/gen-x-y-and-z/how-media-habits-differ (consumer study finding that "gen Z" (16-19-year-olds) is "more averse to advertising in general").

[302] Richardson v. Buhl, 77 Mich. 632 (1889).

The fact that this century's new communications utility is free but necessitates widespread surveillance of consumers is a paradox in a democracy. Facebook watches, monitors, and remembers what over 2 billion people do and say online. Contrary to what those in the advertising industry would regulators to think, American consumers value a state of no surveillance and have attempted to protect this aspect of their privacy since the beginning. The fact that the free market today offers no real alternative to this exchange is a reflection only of the failure of competition.

At least for this titan of tech, antitrust law provides a framework for appreciating and correcting for the foreclosure of consumer choice. Facebook is a monopoly that tipped the early market with promises of data privacy and then engaged in a long line of misleading conduct, which foreclosed competition. The historical record tells the story of Facebook's monopoly power in the social media market. Facebook tried, but could not, degrade the quality of its product to impose commercial surveillance on users through Beacon in the competitive market of 2007. Thereafter, Facebook pivoted to licensing Like buttons, Logins, and other products to independent businesses, which Facebook could leverage for the same purpose. Yet competition between 2008 and 2014 continued to restrain Facebook's ability to initiate tracking for the purpose of targeted advertising. Facebook had to retreat from alleged accidental tracking, assure consumers and other market participants that the underlying code for social plugins was not used for commercial surveillance, and then promise users an ability to vote on future privacy changes. Only after the exit of competitors, and the barrier to entry that comes with over a billion users on a closed communications protocol, was Facebook able to reverse course. The history of Facebook's market entry and subsequent rise is the story of Facebook's monopoly power.

Facebook's pervasive and intrusive commercial surveillance of citizens' digital footprints is merely this titan's form of monopoly rents.

Consumers today turn from Facebook to other websites and apps and face an identical degradation of quality across millions of sites and competitors on the advertising side of the market. For publishers like *The New York Times* and others, Facebook extracts commercial surveillance of their customers through publishers' licenses of Facebook's business products (e.g., Like buttons etc.). Facebook has commoditized these publishers' own user data, once a prized proprietary possession, for its own benefit either to sell Facebook advertising or the advertising of a publisher's competitors. This market structure has deteriorated the pricing power of market actors across the horizontal market and resulted in the duopoly of Facebook and Google—which account for just about the entirety of the growth in the digital advertising market against a backdrop of publishers such as BuzzFeed or The Guardian soliciting reader donations.

The historical record that elucidates Facebook's monopoly power raises the question of whether Facebook's decade-long course of conduct was anticompetitive—especially in the winner-take-all market of a closed communications platform. The record is replete with reliance-inducing future promises, false statements, disingenuous excuses, and convenient omissions which, collectively, likely deceived users. The adoption of a user referendum process for future privacy changes coupled with the failure to meaningfully notify users of an opportunity to vote further raises the specter of a pattern of anticompetitive conduct. Indeed, the wider record of misleading and deceptive conduct—whether that conduct was the subject of an FTC or congressional investigation or the complaints of advertisement buyers—may point to a more systemic problem which harms not only consumer welfare but also presents risk to market stability. Antitrust scholar Robert Steiner once warned that deception by a dominant firm could have a domino effect within an industry, leading smaller firms to engage in similar patterns of

conduct and inefficiency in the industry.[303] Indeed, today, the digital advertising industry is considered one of the most fraud-stricken in the world—the industry expects to absorb $19 billion of waste due to fraud in 2018.[304]

To correct for consumer harm and reduction of choice in the market, a remedy must induce competition and stop horizontal coordination. To induce viable opportunity for new entrants, consumers must be able to export their social graph,[305] and Facebook should migrate from a closed to an open communications protocol. A user on Facebook should be able to send a message to, or receive a message from, a user of a competitive social network—in the same way that users of AT&T can call or text a user of Sprint, Verizon, or T-Mobile. The adoption of an open application programing interface for user messages, chats, posts, and other communications could aid this process. The social network LinkedIn permits communications to be distributed across users' Twitter feeds for example. Additionally, it is paramount that a remedy put a stop to coordination amongst competitors. For this, we need to empower consumers with a singular Do Not Track switch that can counter the collusion in the horizontal market. Consumers must be able to just say no to commercial surveillance—a broad interconnected apparatus that uniquely

---

[303] Robert L. Steiner, *Double Standards in the Regulation of Toy Advertising*, 56 CINCINNATI L. REV. 1259, 1264 (1988). S*ee also* Eastman Kodak Co. v. Image Tech. Servs., Inc., 504 U.S. 451, 474 n.21 (1992) (noting that "in an equipment market with relatively few sellers, competitors may find it more profitable to adopt Kodak's service and parts policy than to inform the consumers").

[304] ASS'N OF NAT'L ADVERTISERS, THE BOT BASELINE: FRAUD IN DIGITAL ADVERTISING 2017 REPORT (2017), *available* at http://www.ana.net/content/show/id/botfraud-2017?mod=article_inline; Alexandra Bruell, *Ad Fraud Declines Offer Hope as Marketers Fight Sophisticated Bots*, WALL STREET J. (May 24, 2017), https://www.wsj.com/articles/ad-fraud-declines-offer-hope-as-marketers-fight-sophisticated-bots-1495645098?mod=article_inline (economic loss due to fraud estimated at $6.5 billion in 2017); *Estimated cost of digital ad fraud worldwide in 2018 and 2022 (in billion U.S. dollars),* STATISTA.COM (2018), https://www.statista.com/statistics/677466/digital-ad-fraud-cost/; Lara O'Reilly, *Google Issuing Refunds to Advertisers Over Fake Traffic, Plans New Safeguard*, WALL STREET J. (Aug. 25, 2017), https://www.wsj.com/articles/google-issuing-refunds-to-advertisers-over-fake-traffic-plans-new-safeguard-1503675395; Suzanne Vranica, *P&G Contends Too Much Digital Ad Spending Is a Waste,* WALL STREET J. (March 1, 2018), https://www.wsj.com/articles/p-g-slashed-digital-ad-spending-by-another-100-million-1519915621.

[305] Others, including economist Luigi Zingales and Guy Rolnik, have also advised for social graph portability to increase competition. Luigi Zingales & Guy Rolnik, *A Way to Own Your Social-Media Data*, N.Y. TIMES (June 30, 2017), https://www.nytimes.com/2017/06/30/opinion/social-data-google-facebook-europe.html.

serves the digital duopoly. While politicians and regulators grapple with how to make sense of current market structures in and consumer frustrations with Big Tech, the principles of antitrust provide clarity for this era's dominant communications platform.