The Center for Growth and Opportunity at Utah State University

Public Interest Comment on the FTC Trade Regulation Rule on Commercial Surveillance and Data Security, R111004

Authors:

Will Rinehart[a]

Taylor Barkley[b]

Aubrey Kirchhoff[c]

Docket ID: FTC-2022-0053

Submitted: November 21, 2022

a Will Rinehart, Senior Research Fellow, The Center for Growth and Opportunity at Utah State University
b Taylor Barkley, Technology and Innovation Director, The Center for Growth and Opportunity at Utah State University
c Aubrey Kirchhoff, Technology and Innovation Program Associate, The Center for Growth and Opportunity at Utah State University

The Center for Growth and Opportunity at Utah State University

Executive Summary

The Federal Trade Commission (FTC) through this ANPRM is pursuing a topic of immense importance to the American public and economy. Indeed, if the agency moves to an NPRM, it is likely to go beyond its authority. Congress would be better suited to provide guidance, which the Commission could then implement.

There are 7 takeaways for the FTC in the following comments:

- Commercial surveillance is a novel and broad term that encompasses a wide variety of practices, both legitimate and illegitimate;
- Using it as a basis for sweeping rulemaking will fail to accurately capture the complexity of the online data collection marketplace and risks wiping out the benefits of the online platform infrastructure;
- Multisided platforms are unique because they bring together two groups for their mutual benefit;
- Firms are likely to create privacy policies that satisfy the average or marginal user, meaning that consumers aren't as biased in their decision-making as is assumed;
- Privacy creates costs disproportionately impacting the revenue of small and direct-to-consumer businesses and limiting safe and competitive options for younger users;
- Leaders should be skeptical that a particular technique can solve the bias-variance problem; and
- Lastly, algorithmic decision-making typically has a comparative advantage over human decision-making.

In the end analysis, many of the questions in this ANPRM rest on fundamental assumptions that are still debated and remain unresolved. However, if the FTC does pursue a rule, there will be costs that could easily outweigh the benefits.

Introduction

The Federal Trade Commission (FTC) through this ANPRM is pursuing a topic of immense importance to the American public and economy. Indeed, if the agency moves to an NPRM, it is likely to go beyond its authority.

For one, the term employed—commercial surveillance—is a wholly new term that has never been explored by this Commission. In the past, the Commission has explored privacy and information harms, but now, the Commission appears to be reframing the debate by seeing all collection as surveillance. This kind of rhetorical move, however, forces the agency into a vice because it sets the terms of the debate. A world where all collection is presumed harmful is one where consumers eventually lose out.

The FTC is correct to ask about harmful business practices and commercial incentives that could harm consumers (Question 11). However, this is best done on a case-by-case basis and not in sweeping terms. Indeed, case-by-case investigation and adjudication is where the FTC shines. Here the agency moves beyond its scope by asking a question far too broad for regulatory rules. The market and competitive pressures are, for the most part, keeping commercial interest in line. Consumers face a wide array of choices between price and quality. Firms are aware of these pressures, and, to the extent that they are not, they are likely headed for failure.

Over the course of this ANPRM, the FTC assumes consumer harm when consumer behavior says otherwise. Again, the agency should approach harms on a case-by-case basis, especially in the case of minority populations. Research and the market above all show that consumers value and derive benefit from services and products the agency says participate in "commercial surveillance." The will of consumers should be of significant importance to the FTC.

Specifically, when it comes to consumers under the age of 18 and 13, the FTC is pursuing an important line of inquiry. With its current COPPA authority, this is one area where the agency has some expertise and track record. However, the set of questions asked by the agency is so wide-ranging that it is not wise to pursue rulemaking at this moment. Instead, the agency should continue to learn from researchers about the best methods of guaranteeing minors are not harmed online. It should also not assume that all commercial dealings with minors are inherently negative and harmful.

Lessons from COPPA since 1998 indicate costly rules limit safe and competitive options for users under 13. More research should be done in this nascent and fast-changing area while relying on non-governmental groups for solutions and protections from harm for minors.

The FTC is also entering into a set of issues where government agencies have already done valuable work, in particular, the National Institute of Standards and Technology (NIST). A voluntary framework is already in place that was the result of private and public collaboration. Rather than create regulation anew, the FTC should look to colleagues and efforts in other federal agencies to ensure there is adoption of these practices.

Finally, on the topics of algorithmic bias and automated decision-making, the harms are as real as the benefits, but the benefits are often underrated. The scope of the FTC's questions in the ANPRM seem to hint at this dynamic. If the FTC is concerned about indiscernible bias in decision-making, they should be concerned about decision-making among human beings. This is not to wave away concerns or say they do not exist. Rather, it is to take into account the reality that

algorithmic decision-making can aid human decision makers and, unlike human beings, is auditable, especially when deployed by governments, and malleable.

These comments are meant to guide the FTC as it examines these important issues. The Commission serves an important role in protecting consumers. However, the agency neither has the legal authority nor the evidence on its side to embark on broad rulemaking. The FTC would do well to abandon this process and await direction from Congress.

The FTC should only implement a bill that Congress sent it

(Questions 7–10, 62–64, 71–72)

The current ANPRM is a scope shift for the Federal Trade Commission (FTC). Previous efforts at protecting consumer data focused on privacy harms and informational injuries. The line of questioning pursued by this notice, however, suggests that the agency is considering a significant scope expansion with the intent to regulate privacy through trade regulation rules. Harms and injuries aren't the focus, anymore. Instead, the mere conduct of commercial surveillance is being called into question.[1]

The agency should tread carefully. The totality of the questions and the framing of the notice of an upcoming "Trade Regulation Rule on Commercial Surveillance and Data Security" suggests that the agency wants to make some conduct per se illegal through a rule. But unlike Children's Online Privacy Protection Rule (COPPA) or the Gramm-Leach-Bliley Act, which were written by Congress and then enforced by the FTC through a rule, the agency seems poised to establish rules without any enabling legislation. For legal and practical reasons, Congress should be setting the rules for consumer privacy. If the FTC were to adopt rules that fit the criteria laid out in the ANPRM, the agency is likely to move beyond its authority.

Practically, Congress is the better venue for crafting rules of such a potentially sweeping impact. Indeed, Congress is currently proceeding with various legislative attempts to craft consumer privacy laws. These laws are being crafted via the legislative process of public hearings and input from stakeholders, all overseen by popularly elected officials representing the diverse American public. The FTC holds none of these strengths or capabilities that have a higher chance of striking the right balance.

Congress clearly delineated the scope of the FTC's rulemaking authority in the Federal Trade Commission Improvement Act.[2] Even if the FTC had the clear authority to craft rules that impact wide swathes of the economy, doing so through Congress is likely to achieve a better result. Impatience over congressional inaction is not an excuse for the FTC to usurp congressional authority.

---

1 Press Release, *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations,* Federal Trade Commission (Aug. 29, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

2 Lawrence J. Spiwak, *Phoenix Center Policy Bulletin No. 59*, Phoenix Center (Sept. 2022), https://www.phoenix-center.org/PolicyBulletin/PCPB59Final.pdf.

Surveillance practices, harms, and informational injury

(Questions 1–6)

The FTC is taking a decidedly new path with this notice. New terms, concepts, theories of harm, and regulatory regimes are being discussed. In part, it seems that the Administration wants to establish and then regulate secure data practices, as they have wanted in the past. But the rubric is new.

With this notice, the FTC is exploring "commercial surveillance," an encompassing term that describes "the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information." With this notice, the agency is hoping to garner input on how to "implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive."[3]

Commercial surveillance is a wholly new idea, but the root term, surveillance, has a history going back to the late 1700s. The term surveillance comes to English from French as a result of the surveillance committees, which were instituted in every French municipality in March 1793. These bodies were tasked with Revolutionary fervor to monitor the actions and movements of suspect persons, outsiders, and dissidents during the Great Terror. The English adopted the term to reference government bodies or agencies engaged in oversight, supervision, and watching, with the intent to jail those who violated norms. Until recently, surveillance was typically tied to a state actor or agent. Local police thus surveil suspects in a similar way that the National Security Administration surveils US citizens through mass collection.[4]

Commercial surveillance is analytically distinct from previous understandings of the term. In commercial surveillance, the state isn't the actor, a company is. The notion owes a debt to the popularization of surveillance capitalism by Shoshana Zuboff who published in 2019 "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power." The energy around this book introduced surveillance capitalism to a wide audience including regulatory authorities who have since adopted the concept of commercial surveillance.[5]

Until recently, commercial surveillance usually referenced camera systems that provided video surveillance.[6] Now, commercial surveillance describes the data economy.

---

3 Trade Regulation Rule on Commercial Surveillance and Data Security, Federal Trade Commission, Advance Notice of Proposed Rulemaking; Request for Public Comment; Public Forum, 87 FED. REG. 51273 (August 22, 2022).

4 Electronic Frontier Foundation, "NSA Spying" (accessed Nov. 16, 2022), https://www.eff.org/nsa-spying.

5 See Milton Mueller, "A Critique of the 'Surveillance Capitalism' Thesis: Toward a Digital Political Economy," *Social Science Research Network* (Aug. 2, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4178467.

6 See GoogleTrends, Interest over Time (2004–present): Commercial Surveillance, (accessed Nov. 11, 2022), https://trends.google.com/trends/explore?date=all&geo=US&q=%22commercial%20surveillance%22.

Zuboff shifted the discussion in defining an inner logic to today's digital firms.[7] They "unilaterally claim human experience as free raw material for translations into behavioral data." Even though some of the data is used to improve service, "the rest are declared as proprietary behavioral surplus, fed into advanced manufacturing processes known as 'machine intelligence' and fabricated into prediction products that anticipate what you will do now, soon, and later."

In the next step of the process, these "prediction products are traded in a new kind of marketplace for behavioral predictions that I call behavioral futures markets," allowing surveillance capitalists to grow "immensely wealthy from these trading operations, for many companies are eager to lay bets on our future behavior."

But if the FTC follows this logic, the analysis will be incomplete. Fundamentally, the notion of commercial surveillance conflates two different kinds of data production. In the case of Facebook, Instagram, TikTok, and Twitter, data is produced as a result of the interaction between the user and the platform. If users didn't interact on Facebook, there would be no data to collect and analyze. For sake of clarity, this might be understood as endogenous data but it is sometimes called first-party data.

On the other hand, there are some businesses, broadly known as data brokers, that collect data and sell it without having a direct interaction with the user. Because the data is created outside of a primary interaction, it is best to understand this as exogenous data or third-party data. The FTC seems poised to regulate these kinds of firms and recently filed suit against Kochava Inc.[8]

While the separating line between the two is fuzzy, consumers will react differently when exogenous data creates a cost as compared to endogenous data. If a data broker collects data about you and creates a cost, for example, there is a low likelihood that you will see it and be able to change your actions in response. However, if you face some cost because you went on Instagram and interacted with the platform, you will likely change your actions.

Still, the FTC shouldn't lose sight of the real reason why privacy is important. Data disclosures can create harm. And consumers need to be protected from those costs and harms. Even so, privacy harms are often difficult to ascertain because privacy itself is a nebulous term.

Privacy is an essentially contested concept.[9] It evades a clear definition and when it is defined, scholars do so inconsistently.[10] Warren and Brandeis (1890) describe it as the right to protect someone's personal space and the right to remain alone. Westin (1967) understood it as the right to control personal information. More recently, Schoeman (1992) defined the idea as the right to dignity, autonomy, and ultimately human freedom, while Nissenbaum defined it contextually. Especially in a digital world, there are fuzzy boundaries between the self and the others, between

---

7 See generally William Rinehart, "Zuboff's definition of surveillance capitalism in "The Age of Surveillance Capitalism" commits a category error, a crucial misstep in understanding platform technologies," (Jun. 16, 2020), https://www.williamrinehart.com/2020/zuboffs-the-age-of-surveillance-capitalism-raw-notes-and-comments-on-the-definition/; also see generally William Rinehart, "The Social Dilemma and the Naming/Knowing Dichotomy," (Oct. 19, 2020), https://www.williamrinehart.com/2020/the-social-dilemma-and-the-naming-knowing-dichotomy/.

8 Press Release, *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations,* Federal Trade Commission (Aug. 29, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

9 See Deirdre K. Mulligan, Colin Koopman, and Nick Doty, "Privacy Is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy," *Philosophical Transactions. Series A, Mathematical, Physical, and Engineering Sciences* 374, no. 2083 (December 28, 2016): 20160118, https://doi.org/10.1098/rsta.2016.0118.

10 See Adam D. Moore, "Defining Privacy," SSRN (Jan. 6, 2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1980849

private and shared information. Because of this, "personal preferences play a key role in determining those actions that people cite as violations."[11]

The FTC has the chance to help consumers, but only if the Commission focuses on consumer harm.[12] Medical identity theft, doxing, and disclosure of sensitive medical information, sexual orientation, or gender identity have all been cited by the Commission as places with the potential for harm.[13] As with everything the Commission does, the first focus should be on consumer harm.

The case of *Spokeo v. Robbins* has begun to define the bounds of harm. The *Spokeo* case stems from a dispute over an online profile by Spokeo, a company that aggregates data on people from both online and offline sources.[14] Thomas Robins sued the company claiming they included inaccurate information in his online profile, which violated the Fair Credit Reporting Act (FCRA). Spokeo had indicated that Robins was wealthy, married, in his 50s, and worked in a technical field. Because none of these characteristics are correct, Robins claimed that it limited his ability to get a job.

The district court dismissed Robins' case, claiming that he could not show any actual harm from Spokeo's inaccurate information, and thus didn't have standing. There was logic to this ruling. Robins filed a no-injury class action suit, alleging that the harm came not from some particular injury, but because Spokeo had violated the FCRA statute. After an appeal, the case found itself at the Supreme Court.

Justice Alito wrote the 6–2 decision which instructed the lower court to again review the issue of standing. As the opinion explained, Robins needs to have an "injury in fact" that is both "concrete and particularized." To bring a class action suit, there has to be a concrete injury even if there is a statutory violation. The Court further noted that a concrete injury isn't necessarily synonymous with a tangible one. Indeed, "intangible injuries can nevertheless be concrete." Yet, the Supreme Court didn't go so far as to define the boundaries of these concrete, yet intangible, harms.

The problem of defining harm is one of the most important in privacy law, and so the tangible and intangible distinction matters.

The courts are split on this question. For the First and Third Circuits, these kinds of hypothetical harms to identity theft aren't actionable.[15] The Seventh and Ninth Circuits have recognized allegations of future harm, but even then they are limited.[16] The judge in the Ninth Circuit case noted, "Were Plaintiffs-Appellants' allegations more conjectural or hypothetical—for example, if no laptop had been stolen, and Plaintiffs had sued based on the risk that it would be stolen at some point in the future—we would find the threat far less credible."[17]

The FTC lost their case against LabMD, which was before their own administrative law judge, in part because of this issue. As the judge noted, the FTC's enabling statute "requires proof of something more than an unspecified and hypothetical 'risk' of future harm," yet the agency was

---

11 See Alessandro Acquisti, Curtis Taylor, and Liad Wagman, "The Economics of Privacy," *Journal of Economic Literature* 54, no. 2 (June 2016): 442–492, https://www.doi.org/10.1257/jel.54.2.442

12 *FTC Informational Injury Workshop: BE and BCP Staff Perspective*, Federal Trade Commission, (Oct. 2018), https://bit.ly/3g6HXZC.

13 Press Release, *FTC to Host Workshop on Informational Injury; Seeking Public Comments*, Federal Trade Commission (Dec. 12, 2017), https://www.ftc.gov/system/files/attachments/press-releases/ftc-announces-workshop-informational-injury/public_notice_injury_workshop.pdf.

14 *Spokeo, Inc. v. Robins*, 578 U.S. (2016).

15 See *Katz v. Pershing*, LLC, No. 11-1983 (1st Cir. 2012); see also *Reilly v. Ceridian Corp.*, No. 11-1738 (3rd Cir. 2011).

16 See *Pisciotta v. Old Nat. Bancorp*, No. 06-3817 (7th Cir. 2007); see also *Krottner, et al. v. Starbucks Corp.*, No. 09-35823 (9th Cir. 2010).

17 *Krottner, et al. v. Starbucks Corp.*, No. 09-35823 (9th Cir. 2010).

unable to supply them.[18] Although allegations of future harm are recognized by some courts, in the absence of an actual data breach, lax security methods are not sufficient. Harm needs to be central.

The production of lax data security

(Question 11)

One of the central questions in the ANPRM (Question 11) asks about business models and incentives that could lead companies to practice lax security. Importantly, the Commission wants to know "the checks that companies rely on to ensure that they do not cause harm to consumers."[19] The structures of internet companies, the economies of these platforms, the users, and the market all provide protections for consumers.

Online platforms are unique because their value comes in bringing two or more types of players together. Still, the concept of a platform is not new. Video games, credit cards, newspapers, and radio stations are similar kinds of platforms. Indeed, much like Google, the Mall of America is a platform because it brings together shoppers and sellers. What is new is the internet.

By enabling real-time interactions between agents, the internet has facilitated the development of such platforms. Ultimately, platforms are concerned with how the price is set for each side optimally.

Platforms generate value from two sources. Platform usage externalities are benefits both sides receive when they use the platform. The majority of these savings are due to reduced transaction costs. Restaurant reservations can be made more convenient by using platforms like OpenTable so the customers benefit. Similarly, a restaurant can also save time and money by using an online reservation system.

The second source of information comes from the total number of users on each side of the platform. Network effects are responsible for these membership externalities. When more users join one side of the platform, the value created for them can increase, sometimes exponentially, up until a point when the value drops off.

Andrew Chen, who worked on Uber's rise, describes it through an S-curve with two points of change. The first point of interest is what he calls the "Allee threshold."[20] The name comes from the first researcher to explain population dynamics, Warder Clyde Allee. In the 1930s, as a professor at the University of Chicago, Allee found that goldfish grow faster and can resist water toxicity when grouped together. "Studies in animal aggregations: Mass protection against colloidal silver among goldfishes" was the first time where numbers have a clear benefit like safety.[21] In the same way, birds flock together to confuse and resist predators, meerkat mobs warn each other of danger, and goldfish do better in groups.

---

18 Press Release, *Administrative Law Judge Dismissed FTC Data Security Complaint Against Medical Testing Laboratory LabMD, Inc.*, Federal Trade Commission (Nov. 19, 2015), https://www.ftc.gov/news-events/news/press-releases/2015/11/administrative-law-judge-dismisses-ftc-data-security-complaint-against-medical-testing-laboratory.

19 *Trade Regulation Rule on Commercial Surveillance and Data Security*, Federal Trade Commission, Advance Notice of Proposed Rulemaking; Request for Public Comment; Public Forum, 87 FED. REG. 51273 (August 22, 2022).

20 Andrew Chen, *The Cold Start Problem: How to Start and Scale Network Effects*, New York, NY: Harper Business, (2021), [hereinafter "Chen (2021)"].

21 Ibid.

The Allee threshold is a tipping point where the value of a network increases.[22] Below it, there is pressure to collapse, to head toward zero. But above it, the network's value grows. But the growth doesn't last forever. The network eventually fills to its full capacity. Eventually, the environment becomes overburdened and a carrying capacity is reached, the second point of change. Once the carrying capacity is reached, the use stabilizes.

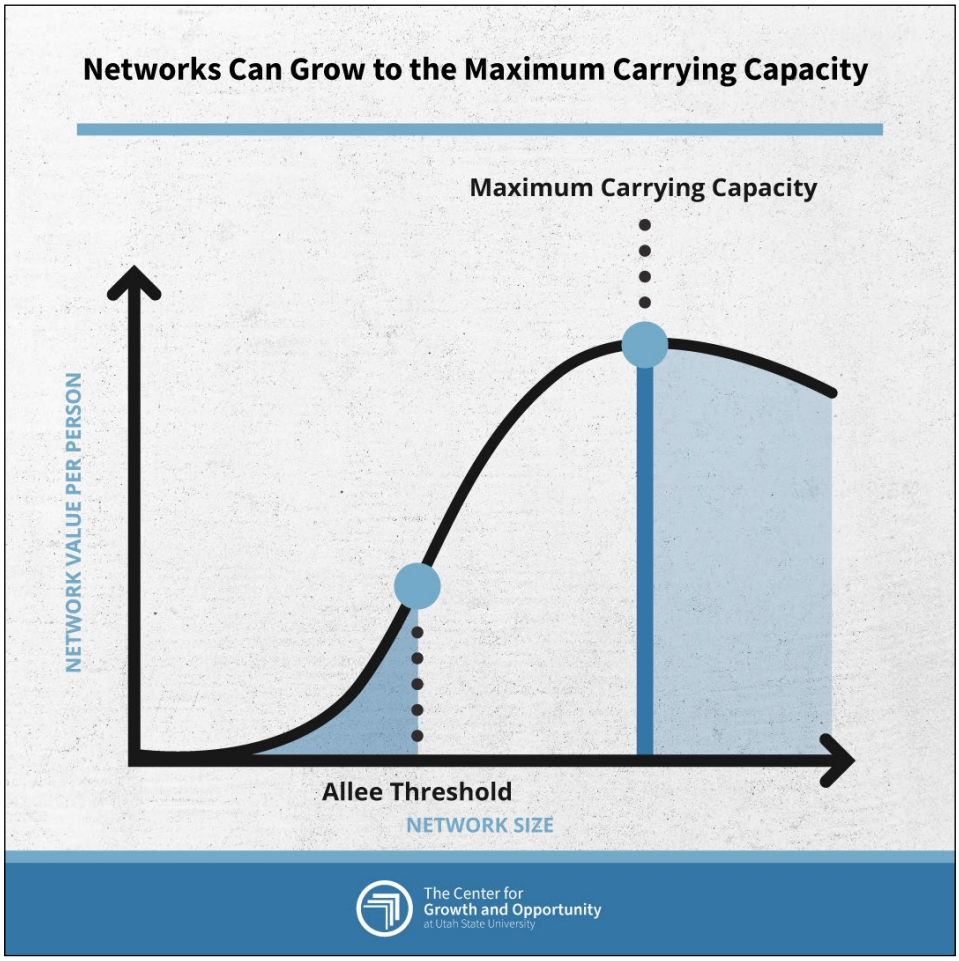

Figure 1: The Allee Threshold

Source: Chen 2021

Networks can backslide easily. Just as it is difficult to get a network started, users will exit or use less of a platform if the price increases or the quality decreases. In this scenario, advertisers also lose interest. A drop in advertiser demand means the entire enterprise becomes valued less. The effect reverberates back to users. Since the platform is less valuable to users when advertisers drop out, there is less content and user demand declines as well.[23]

In cases where demand is tightly integrated, demand is said to have interdependencies. In the formal model, the demand for users is embedded within the demand for advertisers. And the demand of advertisers is embedded in the equation for users. The demand on one side of the market is interdependent with demand on the other.

22 Ibid.

23 Ibid.

The economist Jean Tirole demonstrated that platform prices differ fundamentally from those charged by traditional businesses in his Nobel Prize–winning work in 2003.[24] As Tirole proved, an increase in marginal costs doesn't necessarily lead to an increase in price on that side. In this case, the profit-maximizing price for one side could be below the marginal cost or even negative. Negative prices mean that the consumer receives a benefit for free. [25]

Because demand in a multi-sided market is interdependent, platform operators often find it necessary to take action in order to find an optimal balance of participation between sides of the market. New platforms must achieve, and established platforms must maintain, a critical mass of participants on each side in order to survive. However, demand can deflate rapidly, popping a hole in the value of a platform.

If one side finds its price burden to be too steep, they could leave the platform for a competitor or drop out of the market entirely. As more agents on that side leave the platform, it becomes less attractive to the other side, who may also decide to leave the platform, causing a cycle of declining demand for the platform's services. As more users of each side leave the platform, it risks losing the critical mass of users that supports its success.[26]

Meta seems to be in such a value spiral right now.[27] The value is collapsing to a new normal due to the changes with the 14.5 update of iOS. The loss of user time and advertiser effectiveness has meant that nearly 70 percent of value has been wiped from the books of Facebook and Instagram.[28] This is an issue that current social media juggernauts could eventually face as active user numbers decline.

Something similar happened to Yahoo!'s search engine. It is now generally accepted that Yahoo was running down the quality in the ad side of the market by claiming that some ads were worth more than they were. Advertisers were paying $20 to get a thousand views for pre-roll advertising, which are the ads that appear before a video, but the ads were appearing inside banners in the video, which are typically one-tenth of the price.[29]

As Susan Athey explained, "when Yahoo was under pressure before they shut down their search engine, they basically ran down their quality month by month. . .over a period of three years until their prices went down like thirty percent." Continuing, she explained that "every month they just made things a little bit worse. [Yahoo!] cheat[ed] a little bit and put a little bit of. . .those high value adds on to low value queries." In the case of Yahoo!, which was likely going to be bought regardless, it made sense why the quality dropped: "The numbers look great this month and you don't pay until next month." [30] Users noticed and left the platform.

---

24 Marc Rysman, "The Economics of Two-Sided Markets," *Journal of Economic Perspectives* 23, no. 3 (2009): 124–143 https://www.aeaweb.org/articles?id=10.1257/jep.23.3.125.

25 David S. Evans and Richard Schmalensee, "Failure to Launch: Critical Mass in Platform Businesses, *Review of Network Economics* (Dec. 2010), https://dspace.mit.edu/handle/1721.1/76685.

26 Ibid.

27 Brett Molina and Jessica Guynn, "Facebook is losing users for the first time ever and shared in Meta have fallen off a cliff," *USA Today* (Feb. 3, 2022), https://www.usatoday.com/story/money/2022/02/03/facebook-users-decline-meta-stock/6651329001/.

28 Meta's stock saw a high in 2021 of $376.26. As of the writing, it stands at $113.36; see Google Finance, *NASDAQ: META 5Y* (accessed Nov. 16, 2022), https://www.google.com/finance/quote/META:NASDAQ?sa=X&ved=2ahUKEwjMr6aaj7P7AhVQGVkFHejUDO8Q3ecFegQIFxAY&window=5Y.

29 Michelle Castillo, "Yahoo's troubled advertising business," *CNBC* (Jan. 7, 2016), https://www.cnbc.com/2016/01/07/yahoos-troubled-advertising-business.html.

30 Simons Institute, *Designing Online Advertising Markets*, YouTube (Nov. 20, 2015), https://www.youtube.com/watch?v=jpCXRAboWOc&t=1322s.

It is often assumed that platforms offer a lower-than-optimal level of privacy. But there is no guarantee of that. Although some users may be ill-informed of privacy issues, firms cannot quickly identify these individuals and offer them a separate privacy policy. A company will likely set the quality of service to attract either the marginal consumer or the average consumer depending on the market that the platform is aiming to capture.[31]

At the same time, networks have empowered voices to be critical of the network.[32] A committed minority of individuals might be able to persuade a platform to offer a level of privacy protection above and beyond what the average would want. There is no simple solution to this problem without clear elucidation of the demand interdependencies. It could be that platforms might be setting the level of privacy offerings too high, or they might be setting them too low.

Without further analysis, the FTC cannot easily say whether some commercial incentives and business models are more likely to protect consumers than others. As the next section helps to explain, consumers are far more rational than is often assumed.

The personal consumption of lax data security

(Question 12)

When the FTC is eventually given the authority to act on privacy, it must be careful of the theories in which it roots its action. Conventional assumptions about privacy are being overturned with new research.

Take for example, Ari Ezra Waldman's essay on, "Cognitive Biases, Dark Patterns, and the 'Privacy Paradox.'"[33] In summarizing the literature, Waldman explains that "The rational choice model is ineffective." Continuing, he says, "Individuals have bounded rationality, which limits their ability to acquire all relevant information and translate it into an evidence-based decision. Recent research has identified myriad cognitive and behavioral barriers to rational privacy and disclosure decision-making." The rational choice model, sometimes called the expected utility model, underpins the current regime of privacy regulation, the notice-and-consent regime.

Waldman goes on to highlight three areas where data collection has created problems.[34] First, users are exposed to too much information to make a proper decision about disclosure online. Second, a bevy of cognitive biases skews those choices, even if users have the proper information. And third, dark patterns further distort preferences.

But Waldman isn't the only one who sees bias in decision-making. Researchers David Wilson and Joseph Valacich, for example, say it plainly in the very title of their piece that there is "Irrational

31 Lester T. Chan, "Strong Network Effects Eliminate Spence Distortions," *Social Science Research Network* (Jul. 6, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4203818

32 Elizabeth Nolan Brown, "Libertarian Feminists Ask Facebook to #FreeTheNipple," *Reason Magazine* (June 19, 2015), https://reason.com/2015/06/19/libertarian-feminists-nipple-protest/.

33 Ari Ezra Waldman, "Cognitive Biases, Dark Patterns, and the 'Privacy Paradox,'" *Social Science Research Network* (Sept. 18, 2019) [hereinafter "Waldman (2019)"], https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3456155.

34 Alessandro Acquisti, Curtis Taylor, and Liad Wagman, "The Economics of Privacy," *Journal of Economic Literature* 54, no. 2 (June 2016): 442–492.

decision-making within the privacy calculus."[35] Neil Richards and Woodrow Hartzog,[36] as well as Victor Stango and Jonathan Zinman[37] and others have also singled out bias in privacy decisions.

It is assumed that consumers are making biased decisions, which necessitate regulatory correctives and nudges. Waldman, for example, points out that, "Today, we have too much data, too many data collection pathways, and too much opacity about those pathways." Besides, "if none of these cognitive hurdles to rational disclosure decision-making existed, internet users would still face the limitations imposed on them by design." Website design and UX makes our choices not always reflect what we really prefer. Following this logic, the FTC needs to realign incentives to serve consumers.

Still, the FTC should be cautious in how it understands consumer decisions. Decision theory is often understood as three different kinds of theories. Economics typically concerns itself with *predictive theory*, which has explanatory power in predicting people's choices given a set of options. Predictive theories stand in contrast to a *normative theory*, which is a theory of how people should make decisions, or a *descriptive theory*, which is a theory of how people come to make decisions.

Beginning with the work of Kahneman and Tversky, behavioral economics has been revolutionary to the field because it has shifted the structure of the predictive theories in economics away from rational choice and towards prospect theory.[38] But the advancements in predictive power say little about the kind of preferred decision rules we should adopt i.e., the normative theory. As R. A. Briggs explained in reviewing the literature on rational choice, the normal model of "utility theory makes faulty predictions about people's decisions in many real-life choice situations (see Kahneman & Tversky 1982); however, this does not settle whether people should make decisions on the basis of expected utility considerations."[39]

Waldman, for example, highlights the bias that arises from impatience, and in doing so, tetters on implicitly adopting rational theory:

> Hyperbolic discounting, or the tendency to overweight the immediate consequences of a decision and to underweight those that will occur in the future, makes it difficult for consumers to make rational disclosure decisions. Disclosure often carries with it certain immediate benefits—convenience, access, or social engagement, to name just a few. But the risks of disclosure are usually only felt much later.[40]

Hyperbolic discounting merely means that a person will discount future rewards in a manner best described using the hyperbola curve. The rational assumption is that they should be discounting the future at a linear rate. Within the privacy space, this phenomenon is sometimes called "benefit immediacy."[41]

---

35 David W. Wilson and Joseph S. Valacich, "Unpacking the privacy paradox: Irrational decision-making within privacy calculus," 2021, *International Conference on Information Systems* 5 (2012): 4152–4162.

36 See also Neil Richards and Woodrow Hartzog, "The Pathologies of Digital Consent," *Washington University Law Review* 96, no. 6 (January 1, 2019): 1461–1503, https://openscholarship.wustl.edu/law_lawreview/vol96/iss6/11.

37 Victor Stango and Jonathan Zinman, "We Are All Behavioral, More or Less: A Taxonomy of Consumer Decision Making," Working Paper, National Bureau of Economic Research (November 2020), https://doi.org/10.3386/w28138.

38 Daniel Kahneman and Amos Tversky, "The Psychology of Preferences," *Scientific American* 246, no. 1 (1982) 160–173.

39 "Normative Theories of Rational Choice: Expected Utility," *Stanford Encyclopedia of Philosophy* (last modified Aug. 15, 2019), https://plato.stanford.edu/entries/rationality-normative-utility/.

40 Waldman (2019).

41 David W. Wilson and Joseph S. Valacich, "Unpacking the privacy paradox: Irrational decision-making within privacy calculus," *International Conference on Information Systems* 5 (2012): 4152–4162.

But hyperbolic preferences have been found all over decision-making, not just in privacy. Humans aren't the only animals that exhibit hyperbolic time preferences. Pigeons and rats exhibit time preferences that come close to hyperbolas as well.[42] While the rational choice model had been pervasive in creating an expectation of a certain kind of choice, the reality is that many animals don't choose in a linear fashion. In other words, our models of decision-making are flawed.

Increasingly, researchers are turning to risk-based models because they seem to have both predictive power and normative power. These models just assume that the person is uncertain about the payoff structure and that, over time, people can learn and adapt to it. These two additions help to explain "various core empirical regularities, such as why people often appear very impatient, why per-period impatience is smaller over long than over short horizons, why discounting is often hyperbolic even when the present is not involved, and why choices frequently violate transitivity."[43]

The additions make intuitive sense. Thinking about joining Facebook in 2012 when the company is being praised for its role in revolutions is very different than joining the network now in 2022, sometime after the company was hauled in front of Congress. The payoffs are different. Indeed, many people have learned that they don't like the service and so have left.

Adding these two critical elements to decision-making can be experimentally shown to explain impatience. This research also explains how important context-dependent decision-making is. When the decision environment is more complex, people get more impatient, and they tend to rely upon defaults and experts.[44]

Hyperbolic discounting is one of the key elements cited in the privacy paradox. First coined in 2001, the privacy paradox is a seeming incongruity between people's desire for privacy and their unwillingness to stop using services that might violate that privacy.[45] A cottage industry has sprung up detailing all of the times that consumers say they want privacy, but still choose something else. Another version of this paradox comes in the variation between the willingness-to-pay for privacy and the willingness-to-accept disclosure of it: "In a survey of 2,416 Americans, we find that the median consumer is willing to pay just $5 per month to maintain data privacy (along specified dimensions), but would demand $80 to allow access to personal data."[46] As one review of the literature described it, "While many users show theoretical interest in their privacy and maintain a positive attitude towards privacy-protection behavior, this rarely translates into actual protective behavior."[47]

The academic narrative, however, seems to ignore how consumers actually behave online. According to Blockthrough's March 2021 survey, about 40 percent of US internet users use an ad blocker on any device.[48] At the same time, users actually use ad blockers far less than they say they do, indicating that there is a big discrepancy between user-reported and detected ad-blocked usage.

---

42 George Ainslie, "Specious reward: A behavioral theory of impulsiveness and impulse control," *Psychological Bulletin* 82, no. 4 (1975): 463–496.

43 Benjamin Enke and Thomas Graeber, "Cognitive Uncertainty in Intertemporal Choice," National Bureau of Economic Research (Dec. 2021), https://www.nber.org/papers/w29577#fromrss.

44 Ibid.

45 See Barry Brown, *Studying the internet experience*, Hewlett Packard (Mar. 26, 2001), https://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf.

46 A.G. Winegar and C.R. Sunstein, "How Much is Data Privacy Worth? A Preliminary Investigation," *Journal of Consumer Policy* 42 (Jul. 1, 2019): 425–440.

47 Susanne Barth and Menno D.T. de Jong, "The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review," *Telematics and Informatics* 34, no. 7 (Nov. 2017): 1038–1058.

48 Insider Intelligence, "Consumer attitudes towards digital advertising and ad blocking usage," (Apr. 5, 2022), https://www.insiderintelligence.com/insights/ad-blocking/.

According to AudienceProject, 18 percent of desktop sessions and 7 percent of mobile sessions used an ad blocker in 2020, while 37 percent and 15 percent of surveyed users said they were using one.[49]

The typical understanding of these choices again suggests that people are irrational, but a more nuanced reading would see that there are costs associated with ad blockers that people aren't willing to pay.

A similar reading exists for the privacy paradox as well. A lot of people rightly value their privacy. But there is no privacy paradox if you value the service even higher than the potential cost in privacy. Privacy might be highly, prized but it is often chosen second when it is bargained for a realized good or service.

Research confirms both points. Based on an extensive privacy survey Caleb Fuller conducted, it was discovered that 90 percent of respondents are aware of Google's information collection.[50] At the same time, these services are valued. The median user would require $17,530 to forgo search engines for a year, $8,414 to stop using email for a year, and $3,648 to go without digital mapping technology.[51] My own work suggests that consumers collectively value Facebook to the tune of nearly one trillion each year.[52]

Moreover, the choice overload hypothesis doesn't seem to replicate well. Countless studies have found strong evidence of choice overload in the lab and in the field. But others have found no evidence of choice overload, as well. To help parse the results, Benjamin Scheibehenne, Rainer Greifeneder, and Peter Todd conducted a meta-analysis that combined 63 conditions from 50 published and unpublished experiments (N = 5,036) to estimate the true effect of the choice overload hypothesis. They ended up finding a "mean effect size of virtually zero but considerable variance between studies." As they explained it, "Analyses indicated several potentially important preconditions for choice overload, no sufficient conditions could be identified." Indeed, when you ask people if they feel as though they are inundated with information, users are split about 80–20 with around 80 percent saying that they handle the information.[53]

Experimental economics and developments in decision science both have done much to recover the ground that was seemingly lost. Research in the experimental literature still finds that markets are the most efficient method of exchange of commodities even when key assumptions like complete information don't exist. As economists Omar Al-Ubaydli and John List summarized in a review of this space, "Many behavioral anomalies disappear when traders are sufficiently experienced in their roles, rehabilitating markets' ability to organize the efficient exchange of commodities."[54]

---

49 Ibid.

50 Caleb Fuller, *How Consumers Value Digital Privacy: New Survey Evidence*, Program on Economics & Privacy (Feb. 2018), https://pep.gmu.edu/wp-content/uploads/sites/28/2018/02/Fuller_How-Consumers-Value-Digital-Privacy.pdf.

51 Erik Brynjolfsson, Avinash Collis, and Felix Eggers, "Using Massive Online Choice Experiments to Measure Changes in Well-Being," *Proceedings of the National Academy of Sciences* 116, no. 15 (April 9, 2019): 7250–55, https://doi.org/10.1073/pnas.1815663116.

52 William Rinehart, "Consumers Value Facebook to the Tune of $1 Trillion a Year," The Center for Growth and Opportunity (Jul. 16, 2020), https://www.thecgo.org/benchmark/consumers-value-facebook-to-the-tune-of-1-trillion-a-year/.

53 John B. Horrigan, "Information Overload," Pew Research Center (Dec. 7, 2016), https://www.pewresearch.org/internet/2016/12/07/information-overload/.

54 Omar Al-Ubaydi and John A. List, "Field Experiments in Markets," Poverty Action Lab (Sept. 2015), https://www.povertyactionlab.org/sites/default/files/research-paper/Al-Ubaydli_List_Market_Field_Experiments-2.pdf.

Consumer consent, opt-outs and opt-ins

(Questions 73–82)

Consumers are demonstrating the power of consent in the social media market. New trade regulations in this area are unnecessary. It is incumbent on the FTC to demonstrate the need for new rules in the face of an incredibly dynamic sector where the consumer is king.

The power of opt-in and opt-out choices have been on display throughout 2022. Meta, formerly Facebook, has seen 70 percent of its value erased.[55] More than $230 billion was lost in a day, the biggest one-day loss for any company, ever. While investments in the Metaverse were a part of the drop, the company singled out two headwinds, Apple's iOS 14.5 software update and TikTok.

There is good reason to believe that the massive dip in the stock price can be traced back to Apple's iOS 14.5 update, which was pushed out in April 2021.[56] In this update, Apple rolled out App Tracking Transparency (ATT) regime, which presents users with a popup every time they download a new app. This popup asks them if the app has their "permission to track you across apps and websites owned by other companies."[57]

While Apple has not released official numbers, third-party reports suggested that 80 percent to 95 percent of users were choosing not to be tracked across sites.[58] Without a means to connect all of the pieces together, Facebook is now blind.[59]

Before last year, the ad ecosystem was situated differently. Stretching back to at least iOS 10, which was released in September 2016, iPhone users could opt out of ad tracking. But the factory settings, the defaults, opted-in users to the identifier for advertisers (IDFA) system. This key allows advertisers to compile aggregate data about a user's behavior. Because few people turned it off, Facebook was able to stitch together how the device was being experienced using the IDFA as a key to piece together all of the phone's activity.

Meta's secret sauce for ads is built on the IDFA. Both Facebook and Instagram traditionally have commanded a high price for ads because they were able to connect a lot of dots in the conversion funnel. Default settings meant that they could see outside installs happening, which became a lucrative ad market. Defaults also gave Meta the ability to connect final sales. As ad tech specialist Eric Suefert points out, this granularity drove Meta's ability to personalize ads, which contributed to about 50 percent of ad channel prices.[60]

The addition of ATT in iOS 14.5 shifted the market nearly overnight. Advertisers and marketers immediately took note. By July 2021, it was clear that they could no longer rely on sales conversion

---

55 Barbara Ortutay, "Meta, formerly Facebook, faces historic drop as stock tanks," *AP News* (Feb. 3, 2022), https://apnews.com/article/technology-business-media-social-media-facebook-cf74be789988e7e48f3e2fcdf80ddfa8.

56 See generally "iOS 14," *Wikipedia*, (last modified Sept. 30, 2022), https://en.wikipedia.org/wiki/IOS_14.

57 Jesse Holington, "Apple Backs Down on iOS 14 Ad Privacy After Backlash from Facebook and Game Developers," *iDrop News* (Sep. 3, 2020), https://web.archive.org/web/20200918072136/https://www.idropnews.com/news/apple-backs-down-on-ios-14-ad-privacy-after-backlash-from-facebook-and-game-developers/142386/.

58 Estelle Laziuk, "iOS 14.5 Opt-in Rate – Daily Updates Since Launch," Flurry (Apr. 29, 2021), [hereinafter "Laziuk (2021)"], https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/.

59 Ibid.

60 Eric B. Seufert, "IDFA depreciation is Facebook's Sword of Damocles," Mobile Dev Memo (Jul. 20, 2020) https://mobiledevmemo.com/idfa-deprecation-is-facebooks-sword-of-damocles/.

rates, install numbers, and a range of other data.[61] The loss of the IDFA meant Facebook couldn't connect the threads and show users new business products or retarget ads.

Less precision meant higher acquisition costs.[62] Because they could no longer target specific users, ad buyers would have to show an ad to many more users (spend more money) in order to gain a new customer or convert to a sale. But these buyers are constrained. They've got limited budgets. So instead of spending more money on Facebook and Instagram ads, which already commanded a high price, they shifted their spending to other platforms.

Trade publication MediaPost charted the ups and downs of last year, "Almost immediately after Apple dropped iOS 14.5 last year, ad spend shifted to Android. At one point in the summer, the report notes that iOS ad spending fell 32 percent. Since then, it has largely recovered, but there is still some way to go to get back to the pre-ATT era."[63]

Less demand meant ad prices got driven down across Instagram and Facebook.[64] From an apex in mid-2021 at $14.84, the cost per app install is down to $1.28. The cost per impression is down as well, 42 percent on Instagram and 41 percent on Facebook. While ad prices have stabilized, they did so at a new price level.

Privacy and competition tradeoff

(Questions 27–28)

The effect of enhanced privacy rules are likely to disproportionally affect small businesses. Context matters, however, so each case will need to be considered on its own. That being said, the iOS 14.5 changes help to illustrate what could happen if stricter laws are applied to companies.

As the revenue numbers were being unveiled, Eric Benjamin Seufert, wrote a series of technical pieces explaining why the ad dollars wouldn't simply shift towards other platforms.[65] Yes, some ad buyers did head elsewhere, but the 14.5 update meant that a lot of businesses enabled by Facebook and Instagram are just no longer viable. Such a shift is likely to happen with broad privacy rules as well.

To make his point, Seufert walks through some reasonable but hypothetical numbers for a game app, both before and after the 14.5 change. Let's also assume that this company, following many others online, has a power law for its total lifetime value (LTV) "with 95 percent of users spending $0 in their lifetimes."[66] This means that there is a skew between the average revenue per user (ARPU) and the average revenue per paid user (ARPPU), which comes from the long right tail.

---

61 Kurt Wagner, "Facebook Users Said No to Tracking. Now Advertisers are Panicking," *Bloomberg* (Jul. 14, 2021), https://www.bloomberg.com/news/articles/2021-07-14/facebook-fb-advertisers-impacted-by-apple-aapl-privacy-ios-14-changes#xj4y7vzkg.

62 Patrick McGee, "Snap, Facebook, Twitter and YouTube lose nearly $10bn after iPhone privacy changes," *Financial Times* (Oct. 31, 2021), https://www.ft.com/content/4c19e387-ee1a-41d8-8dd2-bc6c302ee58e.

63 Laurie Sullivan, "Apple Search Ads Network Up 33% Since Introduction of iOS 14.5, Report Finds," Media Post (Feb. 8, 2022), https://www.mediapost.com/publications/article/370992/apple-search-ads-network-up-33-since-introduction.html?utm_source=newsletter&utm_medium=email&utm_content=headline&utm_campaign=125217&hashid=dGEvnTIdR-mRVtQ1KpZ97w.

64 See Average Cost Per Install on Facebook Ads (Oct. 2021–Oct. 2022), Revealbot, https://revealbot.com/facebook-advertising-costs/cpi-cost-per-install-mobile-app.

65 Eric B. Seufert, "How does IDFA depreciation impact ad prices?" Mobile Dev Memo (Aug. 24, 2020) [hereinafter "Seufert (2020)"], https://mobiledevmemo.com/what-happens-to-ad-prices-when-the-idfa-is-deprecated/.

66 Ibid.

So what happens once ad personalization declines due to the change? For one, the top-of-funnel marketing metrics lose their precision, so relevant high-value audiences aren't reached as often. The result is that fewer people go through the conversion funnel.[67] At the same time, all of the down-funnel metrics degrade as well. So the entire value distribution shifts and declines, since there aren't as many paying users. ARPU and ARPPU both decrease, and combined, "the underlying economics for the advertiser change in a way that reduces the viability of ad spend."[68]

One of the lessons Seufert tries to impart from his own experience in the industry is about disproportionality. "If top-of-funnel marketing metrics decrease even slightly, the CPM decrease needed to compensate for the lack of conversion is disproportionately large." Again, using some common numbers in the industry, he was able to show how a 10 percent decline in ad precision had an outsized impact, reducing ad margins by 78 percent. In other words, "If ads are less personalized, not only will fewer users survive the marketing funnel, but those that do will likely monetize to a lesser degree as a result of the loss of precision in targeting."[69]

In other words, ad dollars don't shift elsewhere because it was the precision that allowed the business to pop up in the first place. Not surprisingly, direct-to-consumer (DTC) brands online, which have typically been small operations, have suffered the most. They use precision ads to build brands. As Mike Faber of Spree said, "The times of independent DTC brands might be coming to a painful end."[70]

Seufert concludes by stressing that local context matters,

> This dynamic obviously most impacts apps that are dependent on high-monetizing users that subsidize non-spenders and low-monetizing users. Apps that have a more balanced distribution of LTVs, with less extreme monetization at the high end, will be less impacted by the loss [due to 14.5] for ads personalization, presumably because they are more broadly appealing and less dependent on reaching very specific segments of users.[71]

In reality, the declines were much steeper than 10 percent. Patrick Coddou, the Founder and CEO at Supply, chronicled on Twitter what his clients were saying about the change:[72]

- "...our overall marketing performance has declined by ~40% starting on Monday, 6/21 and continuing through today (6/28)."
- "We are heavily reliant on FB, and the results we're seeing reported in-platform are very, very bad (CPAs skyrocketing up 100%+ what they were a month ago)."
- "Nothing is working. We know very well what audiences and creative perform for our brand. We have been doing this for years. We know the problem is on the Facebook side."
- "June has been terrible. Seeing over 60% drop in revenue."

---

67 Conversion Funnel, Oberlo (accessed Oct. 13, 2022), https://www.oberlo.com/ecommerce-wiki/conversion-funnel.

68 Seufert (2020).

69 Ibid.

70 Make Faber, "Hard times ahead for DTC eCommerce and the rise of a dropshipping marketplace," *Spree Commerce* (Feb. 17, 2022), https://spreecommerce.org/hard-times-ahead-for-dtc-ecommerce-and-the-rise-of-a-dropshipping-marketplace/.

71 Seufert (2020).

72 Patrick Coddou (@soundslikecanoe), Twitter (Sep. 20, 2021, 8:54 PM), https://twitter.com/soundslikecanoe/status/1440117178997510146.

- "Facebook/Instagram Cost Per Acquisition is up triple digits and spend is down 90% from peak in March. Total revenue across the entire business is down 40% from March highs"
- "Our store traffic hasn't recovered post-iOS14 updates. It's insane the drop we've seen in the last three months."
- "Seriously halted us and sick to my stomach daily. Living the American dream to nothing right now. 5-figure spend daily, to absolutely being off the platform because of it."
- "A consistent drop since mid-June with no recovery yet."
- "Our revenue is down 40% this month. Went from very stable cash flowing to hemorrhaging $40k+ per month in our projections. We also barely have runway to make the holidays at this pace. Needless to say, I've been pretty much living in a panic attack for the last two weeks."

But the changes that came with 14.5 only restrained Apple's ecosystem, not the wider market. As the blog Transparency Matters explains of the App Tracking Transparency regime, the name for the 14.5 change that affected Meta:[73]

> App Tracking Transparency made no difference in the total number of active third-party trackers, and had a minimal impact on the total number of third-party tracking connection attempts. We further confirmed that detailed personal or device data was being sent to trackers in almost all cases.

It is a tale about the impact of data regulation. It charts out what will happen if the rules change for data collection and dissemination. Everyone desires privacy and wants their data to be secure in the abstract. But this sense of security comes with a real cost. The cost to marketers and online businesses may be unseen by most, but it still exists nonetheless.

In law and policy circles, it is not uncommon for someone to say that privacy laws spark innovation. But the changes brought with 14.5 cuts against this folk theory of the world. There are disproportionate costs. So, the specifics of privacy law are important, especially since changes in data collection have asymmetric impacts on different industries and players within those industries.

Teens and children

(Questions 13–23)

The safety and health of children is of great importance. Indeed, the FTC has a rich history of enforcing against harmful behavior towards children. However, given the lack of solid evidence connecting advertising and harm for children and the FTC's own findings on advertising directed at children, the FTC should proceed with extreme care on these questions.

The impact of advertising on children is a well-studied, but not well understood subject. Research into this topic surged in the late 1970s when the FTC proposed a rule that would ban advertising

73 Johnny Lin and Sean Halloran, "Study: Effectiveness of Apple's App Tracking Transparency," Transparency Matters (Sep. 22, 2021), https://blog.lockdownprivacy.com/2021/09/22/study-effectiveness-of-apples-app-tracking-transparency.html.

to children.[74] At the time of this proposal, Americans had many of the same concerns about the impacts of advertising on children as they do today. Television had become prevalent and children were increasingly being exposed to advertisements in a way they had not been before.

The KidVid advertising regulations considered by the FTC from 1978 to 1981 should offer many lessons and even some answers to the FTC's current list of questions. Over these three years a thorough process was conducted:

> In response to the NPR, hundreds of written comments, comprising more than 60,000 pages, were submitted by a broad range of interested parties, including consumer organizations; individuals in academic, scientific, technical and government positions; broadcasters; product manufacturers; advertising agencies and associations; and individual consumers. Legislative hearings, held in San Francisco and Washington, DC, produced hearing transcripts of more than 6,000 pages.[75]

Ultimately, the FTC adopted the Staff Report recommendation and did not pursue regulations banning advertising for young children.

Nearly every question about commercial surveillance of children and teens in this ANPRM is best addressed ex post and perhaps by agency investigations, not regulations. The first part of question 20, "How extensive is the business-to-business market for children and teens' data?" would be a worthy fact-finding pursuit by the agency. Third party data dealers are not as visible to consumers and therefore not as susceptible to consumer protest or rapid market signals. However, the primary concern is that they are susceptible to unwarranted government surveillance, a problem Congress has not yet fixed.[76]

Crafting regulations ex ante, as the FTC found in the KidVid proceedings of the 1970s, will likely lead to a similar result in the current social media and online context. Although television advertising technology is crude by today's social media advertising technology, it can serve as a useful analog and starting point. Before moving forward on any of these questions, the FTC should conduct a careful examination of its own resources and findings on these issues. Attempts by platforms or the government to better know the age of an audience requires data collection. Collecting data on users presents cybersecurity risks and privacy concerns of their own. Should the agency pursue regulations aimed at protecting children, such regulations, in order to be effective, will require data collection, thus likely putting children and teens at higher risk than the status quo. There are trade-offs.

Although research on the topic surged in the 1970s, these concerns predated television. As early as the 1930s, the topic of targeting advertisements towards children "was an especially sensitive topic that pitted publishers and editors against parents and activists."[77] These events show a trending concern around advertisements towards children that tend to peak when a new medium enters the

---

74 Michelle R. Nelson, "Research on Children and Advertising Then and Now: Challenges and Opportunities for Future Research, *Journal of Advertising* 47, no. 4 (2018) [hereinafter "Nelson (2018)"].

75 J. Howard Beales, "Advertising to Kids and the FTC: A Regulatory Retrospective That Advises The Present," Remarks before the George Mason Law Review 2004 Symposium on Antitrust and Consumer Protection Competition, Advertising, and Health Claims: Legal and Practical Limits on Advertising Regulation (Mar. 2 2004), https://www.ftc.gov/news-events/news/speeches/advertising-kids-ftc-regulatory-retrospective-advises-present.

76 See Press Release, *Wyden, Paul and Bipartisan Members of Congress Introduce the Fourth Amendment Is Not For Sale Act*, (Apr. 21, 2021), https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act-.

77 Steven Holiday, "Jack and Jill Be Nimble: A Historical Analysis of an 'Adless' Children's Magazine," *Journal of Advertising* 47, no. 4 (2018).

mainstream. It would be wise to note this trend and temper any action spurred on by panic until there is a better understanding of the impact that advertising actually has on children.

The current body of literature studying the impact of advertising on children lacks sufficient data on the contemporary forms of media. This is partially due to the inherent difficulties of studying the impact of an industry that has and continues to change rapidly.[78] There is extensive literature on the impact of television advertisements on youth, but much less is known about the impact of newer advertising techniques, such as embedded advertisement.[79]

Currently, there is also a lack of research into the costs and benefits of strict regulations upon advertisements to children. As noted by James Cooper, law professor and former Deputy Director in the FTC's Bureau of Consumer Protection, these regulations have negatively impacted the ability of children's content creators to earn revenue.[80] In a review of COPPA, the Federal Trade Commission estimated that the annual compliance costs for current web services were $6,223, while new services had to pay $18,670. As some have argued, this is a cost worth bearing. On the other hand, the costs crystallize the current industry players and raise the price of entry, thus making disruption all that more difficult.

Despite these clear impacts, the FTC has failed to conduct or satisfy the strict cost-benefit test required by Section 5(n) of the FTC Act as necessary to promulgate new rules regarding the "unfair or deceptive acts or practices." [81] Given the lack of data on the impacts of contemporary advertising techniques on children and without a proper cost benefit analysis, the FTC cannot and should not move forward with rulemaking in this area.

Defaults and standards

(Questions 51–52)

The Commission should encourage the adoption of standards set forth by the NIST concerning data protection. At the same time, the FTC risks overreach if it demands that all companies meet a specific standard.

Again, the Commission should be led by Congress, and Congress could implement a provision similar to that in the Ohio Personal Privacy Act (House Bill 376), which grants companies an affirmative defense against allegations of violations if they create, maintain, and comply with a written privacy program in accordance with the NIST's privacy framework.[82]

The guidelines set forth by the NIST in "NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0" are adaptable to an organization's size and role within the data processing ecosystem, making it an effective common guideline.[83] In drafting

78 Nelson (2018)

79 Steffi De Jans et al., "Advertising targeting young children: an overview of 10 years of research (2006–2016)," *International Journal of Advertising* 38, no. 2 (2019).

80 Techpolicy, *Children's Privacy in Review: The Future of COPPA*, YouTube (June 15, 2022), https://youtu.be/HkEhIyELtQY?t=1608.

81 Alden Abbott, "Potential Rulemaking on Commercial Surveillance and Data Security: The FTC Must Use Cost-Benefit Analysis," TOTM Symposium: FTC Rulemaking on Unfair Methods of Competition, Sept. 7, 2022), https://truthonthemarket.com/2022/09/07/potential-rulemaking-on-commercial-surveillance-and-data-security-the-ftc-must-use-cost-benefit-analysis/.

82 Enact Ohio Personal Privacy Act, OH HB376 (re-referred Feb. 22, 2022).

83 See generally National Institute of Standards and Technology, "NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0," (Jan. 16, 2020), https://csrc.nist.gov/publications/detail/white-paper/2020/01/16/nist-privacy-framework-version-10/final#pubs-documentation.

the NIST Privacy Framework, there was a concerted effort to collaborate with private and private sector stakeholders to create a set of standards that are relevant and not overly burdensome on enterprise. In addition, the NIST maintains transparency through a development archive allowing businesses and private citizens to understand the logic behind every decision. For these reasons, the NIST's Privacy Framework should set the standard for best practices.

Algorithmic bias

(Questions 53–57)

Bias has a specific meaning that is best understood in a simple calculation. Let's say we have a group of people and estimated their height via a statistical model. For simplicity's sake, we know that mean height is 5'10", but our model produced an estimate that said everyone was 6', then the estimate would be biased by 2 inches.

To statisticians, economists, and data scientists, bias has a very specific meaning. Bias is the property of an estimate that describes how far it is from the true value of a population.

In the real world, we often cannot know the true estimate of a population. And so, most classifiers trade-off between bias and another quality, variance. Variance describes the variability of the prediction, the spread of the estimates.

Going back to the example above, if instead of just one estimate of height, we calculated four estimates, and this time, we got 5'8", 5'10", 6', 6'2". In this round of estimates, our average comes to 5'11", which is closer to the 5'10" average. But the variance would be high because we got a range of different estimates that weren't the correct mean. In the real world, bias is often traded for variance.

Indeed, this trade-off is really a subclass of a larger problem that is of central focus in data science, econometrics, and statistics. As Pedro Domingos noted:

> You should be skeptical of claims that a particular technique "solves" the overfitting problem. It's easy to avoid overfitting (variance) by falling into the opposite error of underfitting (bias). Simultaneously avoiding both requires learning a perfect classifier, and short of knowing it in advance there is no single technique that will always do best (no free lunch).[84]

This gets even more complicated when two populations coexist.

When two populations have different feature distributions, the classifier will fit the larger population because they contribute more to the average error. Minority populations can benefit or suffer, depending on the nature of the distribution difference. This is not based on explicit human bias, either on the part of the algorithm designer or on the part of the data collection process, and it is worse if we force the algorithm to be group-blind artificially. So, it is possible that regulations intended to promote fairness can actually make things less fair and less accurate by prohibiting decision-makers from considering sensitive attributes.

Julia Angwin and her team at ProPublica helped to spark a new interest in algorithmic decision-making when they dove deeper into a commonly used post-trial sentencing tool known as

84 Pedro Domingos, "A Few Useful Things to Know About Machine Learning," *Communications of the ACM* 55, no. 10 (Oct. 2012), https://doi.org/10.1145/2347736.2347755.

COMPAS.[85] Instead of predicting behavior before a trial takes place, COMPAS purports to predict a defendant's risk of committing another crime in the sentencing phase after a defendant has been found guilty. As they discovered, the risk system was biased against African-American defendants, who were more likely to be incorrectly labeled as higher-risk than they actually were. At the same time, white defendants were labeled as lower risk than was actually the case.[86]

Superficially, that seems like a simple problem to solve. Just add features to the algorithm that consider race and rerun the tool. If only the algorithm paid attention to this bias, the outcome could be corrected. Or so goes the thinking.

But let's take a step back and consider really what these tools represent. The task of the COMPAS tool is to estimate the degree to which people possess a likeliness for future risk. In this sense, the algorithm aims for calibration, one of at least three distinct ways we might understand fairness. Aiming for fairness through calibration means that people were correctly identified as having some probability of committing an act. Indeed, as subsequent research has found, the number of people who committed crimes were correctly distributed within each group. In other words, the algorithm did correctly identify a set of people as having a probability of committing a crime.

Angwin's criticism is of another kind, as Jon Kleinberg, Sendhil Mullainathan, and Manish Raghavan explain in "Inherent Trade-Offs in the Fair Determination of Risk Scores."[87] The kind of fairness that Angwin aligns with might be understood as a balance for the positive class. To violate this kind of fairness notion, people would be later identified as being part of the class, yet they were initially predicted as having a lower probability by the algorithm. For example, as the ProPublica study found, white defendants that did commit crimes in the future were assigned lower risk scores. This would be a violation of balance for the positive class.

Similarly, balance for a negative class is the negative correlate. To violate this kind of fairness notion, people that would be later identified as not being part of the class would be predicted initially as having a higher probability of being part of it by the algorithm. Both of these conditions try to capture the idea that groups should have equal false negative and false positive rates.

After formalizing these three conditions for fairness, Kleinberg, Mullainathan, and Raghavan proved that it isn't possible to satisfy all constraints simultaneously except in highly constrained special cases. These results hold regardless of how the risk assignment is computed, since "it is simply a fact about risk estimates when the base rates differ between two groups."[88]

What this means is that some views of fairness might simply be incompatible with each other. Balancing for one kind of notion of fairness is likely to come at the expense of another.

Internalizing these lessons about fairness requires a shift in framing. For those working in the AI field, actively deploying algorithms, and especially for policy makers, fairness mandates will likely create trade-offs. If most algorithms cannot achieve multiple notions of fairness simultaneously, then every decision to balance for class attributes is likely to take away from efficiency elsewhere. This isn't to say that we shouldn't strive to optimize fairness. Rather, it is simply important to recognize that mandating one type of fairness may necessarily come at the expense of a different type of fairness.

---

85 Julia Angwin et. al., "Machine Bias," *ProPublica* (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

86 Ibid.

87 Jon Kleinberg, Sendhil Mullainathan, and Manish Raghavan, "Inherent Trade-Offs in the Fair Determination of Risk Scores," Research Gate (Sep. 2016), https://www.researchgate.net/publication/308327297_Inherent_Trade-Offs_in_the_Fair_Determination_of_Risk_Scores.

88 Ibid.

Understanding the internal logic of risk assessment tools is not the end of the conversation. Without data of how they are used, it could be that these algorithms entrench bias, uproot it, or have ambiguous effects. To have an honest conversation, we need to understand how they nudge decisions in the real world.

The benefits of automated decision-making

(Questions 57–61, 65–70)

Algorithms have a range of applications. There are some algorithms, to take one example, that route communications efficiently. But few would cite routing algorithms for bias or false representations. Instead, algorithms can be concerning because they can sometimes reproduce unfair outcomes that deviate from a norm or an expected outcome. It is worth noting that behind every AI is a human doing the tough work of tagging and optimizing outcomes.[89]

Algorithmic decision-making is not perfect, but it is often less biased than human decision-making. Our desire to utilize algorithms should be bolstered by the fact that, even when algorithms and humans produce equally biased results, it is far easier to detect and correct bias in algorithms. With these facts in mind, it is clear that communities that have faced the highest rates of discrimination could benefit the most from the responsible use of algorithmic decision-making. In our journey to reach perfect systemic equality we should not dismiss improvements.

Even with the inadvertent bias introduced by input data, algorithmic decision-making models are often an improvement over human decision-making. In a 2019 study, researchers analyzed mortgages secured by the Government Sponsored Enterprises (GSEs) Fannie Mae and Freddie Mac to test for the presence of discrimination and estimate its level.[90] They found that discrimination was present in both face-to-face decisions and in algorithmic credit scoring. However, FinTech algorithms discriminated 40 percent less than face-to-face lenders.

Yes, false negatives and misinterpretations will happen with credit scores, but are they presumptively illegitimate? It would be a stretch to claim that the previous system of judgmental lending was *more legitimate*. Gender, race, religion, nationality and marital status were implicit factors in decision-making. While it is not perfect, the wide adoption of credit scores has been important in pushing loan decisions towards nondiscriminatory practices.[91] In a study that predates the build-up in housing credit, the implementation of sophisticated risk models was found to be connected to the expansion of home ownership in minority communities, helping it to grow from 34 percent to 47 percent between 1983 and 2001.[92]

Second, it is far simpler to address bias in algorithms than it is in humans.[93] Once the reasons for algorithmic bias are detected, the software can be adjusted. In one such case, the algorithm used healthcare expenditures as a proxy for levels of sickness, thus underestimating the sickness of

---

89 Jonathan Low, "Why Behind Every AI 'Robot" Is a Human," *The Lowdown* (Apr. 17, 2019), http://www.thelowdownblog.com/2019/04/why-behind-every-ai-robot-is-human.html.

90 Robert Barlett, Adair Morse, Richard Stanton and Nancy Wallace, "Consumer-Lending Discrimination in the FinTech Era," Working Paper, National Bureau of Economic Research (Jun. 2019), https://www.nber.org/papers/w25943.

91 Hollis Fishelson-Holstine, "The Role of Credit Scoring in Increasing Homeownership for Underserved Populations," Joint Center for Housing Studies of Harvard University (Feb. 12, 2004), https://www.jchs.harvard.edu/research-areas/working-papers/role-credit-scoring-increasing-homeownership-underserved-populations.

92 Information Policy Institute, *The Fair Credit Reporting Act: Access, Efficiency, & Opportunity The Economic Importance of Fair Credit Reauthorization*, National Chamber Foundation (Jun. 2003), https://www.perc.net/wp-content/uploads/2013/09/fcra_report_exec_sum.pdf.

93 Mullainathan (2019)

black patients since society spends less on them than white patients. Researchers then developed a prototype that adjusted for this reality and made results more equitable. It is far more difficult to alter human bias. Implicit bias training is often offered, or even required, by workplaces, but its impact on improving actual behavior is modest.[94]

Let's be honest. We humans are bad at making decisions. In many situations, we have the same failings that we condemn algorithmic decision-making for having. When a decision needs to be made quickly, humans tend to fall back on their biases and assumptions. Human failings become clear when we consider why algorithms are so often biased.

How should the Commission balance costs and benefits?

(Questions 24–29, 83–92, 95)

The Commission shouldn't be in the business of deciding how to balance the cost and benefits of a privacy law. Congress needs to set out the contours of the rules. But even when the Commission is given the authority to regulate this topic, they should be cautious.

Of all the biases in policymaking, the FTC should be wary of proportionality bias.[95] It is the least talked about, but the most pernicious bias for experts. In short, there is a tendency among all of us to think large events are caused by large actions and small effects have small causes. In the real world, however, causes and effects are rarely of the same proportions. Small actions can shift the equilibrium.

Even something as minor as a ban on personalized advertising can shift the entire market. The United Kingdom's *Online platforms and digital advertising: Market study final report*, compiled by The Competition and Markets Authority, offers evidence to this effect.[96] In a wide-ranging report, the agency dove into data provided by Google on an internal test that the company ran in 2019. In a head-to-head battle between publishers using personalized and non-personalized advertising, Google found that "UK publishers earned around 70 percent less revenue when they were unable to sell personalized advertising but competed with others who could." Small changes can be hugely meaningful.

Additionally, the Commission shouldn't count out the actions of consumers and other market players to pressure. Companies like Dell, Best Buy, Ford, Pottery Barn, Nike, Patagonia, Match and Amazon's video-streaming service, Twitch, have all removed the ability to sign on with Facebook citing concerns with the company's privacy stance.[97]

As noted above in the section on defaults and standards, changes in the defaults can have outsized impacts. But this doesn't just apply to defaults and opt-ins. All laws and regulations have costs and benefits. Indeed, there are an array of privacy laws currently in force at the federal, state, and

---

94 Edward H. Chang et al., "The mixed effects of online diversity training," *Proceedings of the National Academy of Sciences* 116, no. 16 (Apr. 1, 2019): 7778–83, https://www.pnas.org/doi/10.1073/pnas.1816076116.

95 See Aditya Shukla, "Why We Justify Big Events with Big Causes: Balancing Causes with Effects Is an Error," *Cognition Today* (last updated Aug. 15, 2021), https://cognitiontoday.com/why-we-justify-big-events-with-big-causes-proportionality-bias/.

96 *Online platforms and digital advertising*, Competition and Markets Authority (Jul. 1, 2020), https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf.

97 Jonathan Vanian, "The Facebook button is disappearing from websites as consumers demand better privacy," *CNBC* (Sep. 8, 2022), https://www.cnbc.com/2022/09/08/facebook-login-button-disappearing-from-websites-on-privacy-concerns.html.

international levels. Governments and researchers have conducted cost estimates of these existing laws that should provide guidance as the FTC considers the potential costs of a new privacy regulation. The sum total of current economic costs should give pause to the FTC as they consider adding more economic costs. A tally of those costs can be found in the appendix to this filing.

In addition to the real costs, there are privacy costs to poorly written laws. One of the problems with making it easy for consumers to access and delete their data is that it also becomes easy for others to access and delete data.[98] Since the implementation of GDPR, experts have proven it is possible to trick systems designed to comply with the law with the effect of getting someone else's data.[99]

As the above sections show, confirming additional research, the use of digital applications appears to cause consumers to develop their views on privacy.[100] Most importantly, regulators trying to correct this privacy problem will face the impossible task of understanding the optimal privacy level and then adjusting the market to reflect that preference. Even in an ideal world, the best-case scenario will never be achieved. In the end, Congress should be the lead.

98 "To get your personal data, provide more personal data," *FlowingData*, (Jan. 22, 2022), https://flowingdata.com/2020/01/22/to-get-your-personal-data-provide-more-personal-data/.

99 Ibid.

100 Yadong Huang, Chen Long, Shumiao Ouyang, and Wei Xiong, "The data privacy paradox and digital demand," Centre for Economic Policy Research (Jun. 28, 2021), https://cepr.org/voxeu/columns/data-privacy-paradox-and-digital-demand.

Appendix: The cost of privacy legislation

The tables below compile all of the known estimates from researchers and government agencies on the costs created by privacy laws. As policymakers consider different paths, they should be fully cognizant of the costs imposed by these laws.

United States Laws

California Consumer Privacy Act (CCPA)	• CCPA's total compliance cost was estimated at $55 billion, about 1.8% of Gross State Product (GSP), according to a Standardized Regulatory Impact Analysis. • Researchers were uncertain about this estimate, however, and the cost could be as high as 4.6% of GSP. • Between 15,643 and 570,066 businesses were expected to be regulated by the law.[101] • The Information Technology & Innovation Foundation (ITIF) estimates the law "will cost $78 billion annually, with California's economy bearing $46 billion and the rest of the US economy bearing the other $32 billion. California small businesses will bear $9 billion of in-state costs, while out-of-state small businesses face $6 billion of costs."[102] • By analyzing a novel collection of internal data from AI firms, researchers found that the CCPA affords these companies special protection and advantage because of their in-house data. • Firms differ in their ability to collect data internally, depending on their business models and the size of their customer base. • CCPA increases the cost of trading data, causing firms with an inability to collect data in-house or a high reliance on data to see declines in revenue.[103]

101 Berkeley Economic Advising and Research, LLC, *Standard Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations*, Prepared for the California Department of Justice Attorney General's Office California Department of Justice (Aug. 2019), https://web.archive.org/web/20190830173026/http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

102 Daniel Castro, Luke Dascoli, and Gillian Diebold, "The Looming Cost of a Patchwork of State Privacy Laws," ITIF (Jan. 24, 2022), https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/.

103 Mehmet Canayaz, Ilja Kantorovitch, and Roxana Mihet, "Consumer Privacy and Value of Consumer Data," Swiss Finance Institute Research Paper No. 22–68 (Last modified Sep. 6, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3986562.

United States Laws

California Privacy Rights Act (CPRA)	• 66,076 California businesses covered by CCPA are expected to be affected by the regulations of CPRA. • As the state's impact assessment notes, "The proposed regulation has a small cost per business ($127.50) and is thus unlikely to impact entry/exit decisions. . . . We do not expect any jobs to be created or eliminated. . . .The regulation is neither expected to confer competitive benefits nor disadvantages on California businesses." • The cost over its lifetime is pegged to be $8,424,690.[104]
Children's Online Privacy Protection Rule (COPPA)	• When the FTC formalized new rules for COPPA in 2013, they estimated that the "associated labor costs for the 180 new operators potentially subject to the proposed amendments would be $3,360,600 (i.e., $3,285,000 for legal support plus $75,600 for technical support)." Compliance costs for these new operators would be $18,670. • "Similarly, for the estimated 2,910 existing operators covered by the final Rule amendments. . .associated labor costs would total $18,109,900 (i.e., $17,702,500 for legal support plus $407,400 for technical support)." Compliance for this group would cost $6223.33. • "Cumulatively, estimated labor costs for new and existing operators subject to the final Rule amendments is $21,470,500."[105] • In an interview with ZDNET, Perry Aftab, an attorney who helps internet companies comply with COPPA, says she "estimates that it will cost her clients between $60,000 and $100,000 a year to meet COPPA standards. She believes most web sites have accepted the price tag of protecting child privacy online."[106]
Enact Ohio Personal Privacy Act	• According to the Ohio Legislative Service Commission, "Staff of the [Ohio State] Attorney General estimate their annual operating costs of enforcing the bill's requirements at about $556,000, with close to 70% paying for the payroll costs of three full-time staff (two attorneys and one analyst)."[107]

104 State of California Department of Finance, Economic and Fiscal Impact Statement: California Consumer Privacy Act Regulations, STD. 399 (Rev. Dec. 2013), https://cppa.ca.gov/regulations/pdf/std_399.pdf.

105 Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2013)

106 Julia Angwin, "COPPA Cost Too High for Some Sites," ZDNET (Apr. 23, 2000), https://www.zdnet.com/article/coppa-cost-too-high-for-some-sites/.

107 Ohio Legislative Service Commission, H.B. 376 Fiscal Note & Local Impact Statement (Feb. 10, 2022).

The European Union's General Data Protection Regulation (GDPR)

User impacts	• After GDPR, someone exposed to the regulation "submits 21.6% more search terms to access information and browses 16.3% more pages to access consumer goods and services."[108] • "On average, the GDPR's effects on user quantity and usage intensity are negative."[109] • "Comparing long-run equilibria with and without GDPR, we find that GDPR reduces consumer surplus and aggregate app usage by about a third."[110] • GDPR's newly implemented opt-in requirement caused a 12.5% drop in the observed consumers. And the remaining consumers are observable for a longer period of time. Privacy-conscious consumers seem to substitute away from less-efficient privacy protection (e.g., cookie deletion) to explicit opt-out, reducing the pool of short consumer histories. The result is that the average value of the remaining consumers to advertisers has increased, offsetting most of the losses from consumers that opt-out.[111]
Impacts on sites	• A "reduction of approximately 12% in both EU user website pageviews and website e-commerce revenue [was] recorded by the platform after the GDPR's enforcement deadline."[112] • "After the GDPR's enforcement, website use of web technology vendors falls by 15% for EU residents."[113] • "The numbers of total visits to a website decrease by 4.9% and 10% due to GDPR in respectively the short- and long-term."[114]

108 Yu Zhao, Pinar Yildirim, and Pradeep K. Chintagunta, "Privacy Regulations and Online Search Friction: Evidence from GDPR," SSRN Scholarly Paper (Rochester, NY, August 12, 2021), https://doi.org/10.2139/ssrn.3903599.

109 Julia Schmitt, Klaus M. Miller, Bernd Skiera, *The Impact of Privacy Laws on Online User Behavior*, HEC Paris Research Paper No. MKG-2021-1437 (Mar. 16, 2021), https://arxiv.org/pdf/2101.11366.pdf.

110 Rebecca Janßen, Reinhold Kesler, Michael E. Kummer, and Joel Waldfogel, "GDPR and the Lost Generation of Innovative Apps," Working Paper, Working Paper Series (National Bureau of Economic Research, May 2022), https://doi.org/10.3386/w30028.

111 Guy Aridor, Yeon-Koo Che, and Tobias Salz, "The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR," SSRN Scholarly Paper (January 29, 2020), https://doi.org/10.2139/ssrn.3522845.

112 Samuel Goldberg, Garrett Johnson, and Scott Shriver, "Regulating Privacy Online: An Economic Evaluation of the GDPR," SSRN Scholarly Paper (Rochester, NY, July 17, 2019), https://doi.org/10.2139/ssrn.3421731.

113 Garrett Johnson, Scott Shriver, and Samuel Goldberg, "Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR," SSRN Scholarly Paper (Rochester, NY, November 14, 2022), https://doi.org/10.2139/ssrn.3477686.

114 Schmitt, Miller, and Skiera (2021).

The European Union's General Data Protection Regulation (GDPR)

Competitive effects	• Email and display ad marketing channels, which were specifically targeted by GDPR, were the hardest hit industries after the law came into effect.[115] • Smaller vendors were more commonly dropped after GDPR, which increased the relative concentration of the vendor market by 17%.[116] • Although everyone has done worse since GDPR went into effect, Peukert et al. find that Google lost relatively less than everyone else and was significantly able to increase its market share in important markets such as advertising and analytics. • GDPR caused websites to substantially reduce their interactions with web technology providers, even for websites not legally bound by the GDPR. • The researchers also documented an increase in market concentration in web technology services after the introduction of the GDPR.[117] • "Bigger e-commerce firms see an increase in consumer traffic and more online transactions. The increase in the number of transactions at large websites is about six times the increase experienced by smaller firms. Overall, the post-GDPR online environment may be less competitive for online retailers and may be more difficult for EU consumers to navigate through."[118] • After GDPR, EU ventures reduced their monthly deals by 26.1% compared to US venture firms. These effects were more pronounced in the six-month period immediately following GDPR's rollout in 2018, though some lasted up to 12 months.[119] • "GDPR induced the exit of about a third of available apps and in the quarters following implementation, entry of new apps fell by half."[120]

115 Goldberg, Johnson, and Shriver (2021).

116 Johnson, Shriver, and Goldberg (2022).

117 Christian Peukert, Stefan Bechtold, Michail Batikas, and Tobias Kretschmer, "Regulatory Spillovers and Data Governance: Evidence from the GDPR," *Marketing Science* 41, no. 4 (July 2022): 746–68, https://doi.org/10.1287/mksc.2021.1339.

118 Zhao, Yildirim, and Chintagunta (2021).

119 Jian Jia, Ginger Zhe Jin, and Liad Wagman, "The Short-Run Effects of GDPR on Technology Venture Investment," SSRN Scholarly (Last modified May 26, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278912.

120 Janßen, Kesler, Kummer and Waldfogel (2022).

The European Union's General Data Protection Regulation (GDPR)

Compliance cost	• "The average annual budget for compliance with GDPR is $13 million. . . . The budget for organizations with a headcount of more than 25,000 is significantly higher than those organizations with a smaller headcount. However, because of economies of scale, the average per capita budget for organizations with a headcount over 5,000 is $351.59."[121] • According to Gal Ringel, CEO of Mine, a company that helps users reclaim their data, "A single data subject access request (DSAR) and deletion request can cost a company $1,400. This is due to the aggregated total time of the support person, the legal person, and the R&D engineer who needs to go into the database and manually delete information off the servers."[122] • According to a story by Quartz writer Ashley Rodriguez, in a hearing with the US Senate Committee on Commerce, Science and Transportation, "Google's chief privacy officer, Keith Enright, estimated that Google's workforce spent 'hundreds of years of human time' to bring the company into compliance with GDPR." Assuming $72/hr in cost and a minimum of 200 years, the cost for Google's GDPR compliance totaled at least $126 million.[123]

121 Ponemon Institute LLC, *The Race to GDPR: A Study of Companies in the United States & Europe* (Apr. 2018), https://s3-us-east-2.amazonaws.com/mwe.media/wp-content/uploads/2019/04/15202019/Race-to-GDPR.pdf.

122 James Spiro, "Attempting a 'Data Detox' in Today's Digital World," CTech (Aug. 30, 2021), https://web.archive.org/web/20210830083108/https://www.calcalistech.com/ctech/articles/0,7340,L-3916609,00.html.

123 Ashley Rodriguez, "Google Says It Spent 'Hundreds of Years of Human Time' Complying with Europe's Privacy Rules," Quartz (Sep. 26, 2018), Quartz, https://qz.com/1403080/google-spent-hundreds-of-years-of-human-time-complying-with-gdpr.

The European Union's E-Privacy Directive

- After the EU enacted the e-Privacy Directive in 2002, venture capital investments declined by 58 to 75%.[124]

- According to research from Goldfarb and Tucker, when the EU adopted the e-Privacy Directive in 2002, display advertising became far less effective. "The loss in effectiveness was more pronounced for websites that had general content (such as news sites), where non-data-driven targeting is particularly hard to do. The loss of effectiveness was also more pronounced for ads with a smaller presence on the webpage and for ads that did not have additional interactive, video, or audio features."[125]

Limits on Credit Data

- In Chile, a 2012 law restricting information forced credit bureaus to stop reporting defaults, reducing the costs for poorer defaulters while raising the costs for non-defaulters. Overall the law led to a 3.5% decrease in lending and reduced aggregate welfare.[126]

- The availability of digitally verified data significantly expands credit access, as noted by Chan et al.: "The loan origination rate increases by 35.5% on average and is more significant among deep subprime (146%) and subprime consumers (44%). The interest rates charged on these loans rise only slightly. The expanded credit access also benefits lenders, with an estimated 19.6% increase in profit."[127]

- Kim and Wagman looked at variations in local financial-privacy ordinances in five California Bay Area counties. Using data from 2001 to 2006, they compared the effects of stricter privacy laws on mortgage denial rates. Counties with opt-in privacy ordinances experienced lower denial rates for purchase and refinance loans, and counties with privacy ordinances experienced higher foreclosure starts during the 2007–2008 financial crisis.[128]

---

124 Anja Lambrecht, *E-Privacy Provisions and Venture Capital Investments in the EU*, CCIA (Dec. 2017), https://www.semanticscholar.org/paper/E-Privacy-Provisions-and-Venture-Capital-in-the-EU-Lambrecht/12e6c43e51c16787e57b95073aaa283a3e7c56a3.

125 Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising," *Management Science* 57, no. 1 (January 2011): 57–71, https://doi.org/10.1287/mnsc.1100.1246.

126 Andres Liberman, Christopher Neilson, Luis Opazo, and Seth Zimmerman, "The Equilibrium Effects of Information Deletion: Evidence from Consumer Credit Markets," Working Paper, Working Paper Series (National Bureau of Economic Research, September 2018), https://doi.org/10.3386/w25097.

127 Tat Chan, Naser Hamdi, Xiang Hui, & Zhenling Jiang, "The Value of Verified Employment Data for Consumer Lending: Evidence from Equifax," SSRN Scholarly (last modified Oct. 4, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3556554.

128 Jin-Hyuk Kim and Liad Wagman, "Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis," *The RAND Journal of Economics* 46, no. 1 (2015): 1–22, https://doi.org/10.1111/1756-2171.12083.