The Cookie Conundrum: An Investigation Of Consumer Behavior And Online Privacy Regulations

By Gabriel Solis*
solisgab@usc.edu

University of Southern California

Recent regulations, including the European Union's General Data Privacy Regulation (GDPR) and the California Consumer Privacy Act (CCPA), have introduced consent-based mechanisms, such as 'notice and choice,' to enhance consumer privacy rights. While these frameworks focus on obtaining user consent, the role of firm characteristics in shaping consumer decision-making within these mechanisms remains underexplored in existing research. This paper examines whether data-tracking consent mechanisms disproportionately benefit large incumbents over smaller start-ups. Our randomized experiment with 153 participants investigates how firm characteristics affect consumers' willingness to share data. We found directional effects showing consumers tend to trust larger, established firms over smaller ones when making privacy decisions. Our findings highlight challenges in regulating digital privacy, as well-intentioned consent requirements may inadvertently favor incumbents, potentially reducing competition and consumer welfare through increased market concentration.

Keywords: Consent Mechanisms, Brand Trust, Digital Economics, Consumer Decision-Making, Competition

* I would like to express my heartfelt gratitude to my advisor, Alex P. Miller, for his patience and unwavering support throughout this project. His guidance has been instrumental, and I am especially thankful for the countless conversations we had, which deepened my understanding and inspired my work.

Outpacing advances in information technology have significantly disrupted traditional models of privacy, prompting Congress to react and pass legislation aimed at protecting the public while promoting innovation (Agrawal, Gans and Goldfarb, 2019; Brynjolfsson and Kahin, 2002). In today's digital economy, access to technologies like social networks, artificial intelligence (AI), and big data allows firms to process vast amounts of personal data to enhance, market, and sell their products (Goldfarb and Tucker, 2012; Aridor, Che and Salz, 2021). Intangibles such as an individual's traits, online and offline behaviors, photos, and other forms of personal data, while not monetary, have become analogs to currency (Wharton, 2019)[1]. This data collection fuels industries from advertising and e-commerce to healthcare and government sectors. Digital platforms like Google, Facebook, and Amazon, which offer ostensibly free services, generate revenue by leveraging user data to connect consumers with advertisers (Bonatti, 2022).

Data-collecting practices like these naturally raise privacy concerns among consumers. These concerns reflect growing unease about the vast amount of data being collected and the corresponding shift in control over personal information from individuals to organizations. At the heart of this issue is the challenge of distinguishing between what is legally permissible and what is ethically acceptable (Marchant, 2011). In response to public demands, government regulators have proposed and enacted data privacy laws designed to empower consumers with increased transparency and control over the personal data they generate. Among the first was the European Union's General Data Privacy Regulation (GDPR), implemented in 2018, which has served as a blueprint for similar privacy legislation in other countries. The GDPR, among other requirements, mandates that businesses must obtain "consent [which] must be freely given, specific, informed and unambiguous" (Kosta, 2020). Similarly, the California Consumer Privacy Act (CCPA), enacted in 2020, followed this model of transparency and consent.

Broadly, these laws aim to achieve two main objectives: (1) promoting market competition by curbing the dominance of large firms, and (2) mitigating the negative impacts of business activities on individuals and other organizations. However, there is a lack of empirical evidence on how these consent models affect the competitive dynamics of data-intensive industries. Implications of such results

[1]Equally as mentioned in popular press outlets is that "data is the new oil." In other words, data has become a new and lucrative commodity, drawing the interest of regulators (e.g., The Economist "The World's most valuable resource is no longer oil, but data").

suggest that consent requirements in privacy legislation not only fail to effectively regulate leading technology corporations but could also exacerbate existing monopolies and anticompetitive business practices. Existing literature has primarily focused on the effect of different cookie consent interfaces on online users' consent behavior (Utz et al., 2019; Brough et al., 2022; Nouwens et al., 2020; Kim et al., 2019), the impact of privacy regulations on innovation and competition (Campbell, Goldfarb and Tucker, 2015; Bleier, Goldfarb and Tucker, 2020; Johnson, Shriver and Goldberg, 2023; Goldfarb and Tucker, 2019), and the heuristics driving consumer privacy decisions (Acquisti, John and Loewenstein, 2013; Hong, Chan and Thong, 2021; Collis et al., 2021; Chellappa and Sin, 2005).

This paper aims to bridge the gap between these questions. Specifically, we focus on the widespread adoption of consent requirements, particularly the notice-and-choice framework, in privacy laws across the European Union and more recently in the United States. Despite its prevalence in the political discourse on online privacy, the broader implications of the notice-and-choice paradigm remain underexamined. In particular, in how firm characteristics influence consumer decision-making and, in turn, affect market dynamics. To address this, we conduct a web-based experiment that evaluates individuals' propensity to accept or reject a website's cookie policy when presented with varying information about the company. Our findings show that consent decisions are influenced not only by brand affinity (Aaker, 1991) but also by consumers' perceptions of a brand's heritage (Urde, Greyser and Balmer, 2007). Moreover, consumers exhibit limited awareness of prominent privacy regulations and tend to place disproportionate trust in large, incumbent firms over smaller competitors.

The results of our experiment underscore the complexity that comes with regulating privacy. While privacy regulations strive to simultaneously encourage competition and empower consumers, we show that these two goals are at odds under the adoption of consent mechanisms like notice and choice. More broadly, our research highlights that consumer responses to consent requests are highly susceptible to internal, nonnormative biases, which could further exacerbate disparities in the competitive landscape between firms.

In the following sections, we review of the relevant literature on the evolution of privacy laws, the marketing principles that shape consumer decision-making, and key economic theories on privacy. We then present an analysis of our experiment, followed by a discussion of the findings and their implications.

I. Background & Related Work

Privacy is a fluid concept that various disciplines, including law, economics, and marketing, have explored. Legally, the right to privacy is relatively recent, first conceptualized in the late 19th century by Samuel Warren and Louis Brandeis in their seminal article *The Right to Privacy* (Warren and Brandeis, 1890), which framed privacy as the 'right to be let alone.' However, early conceptions of privacy, like those of Warren and Brandeis, do not fully capture the digitized landscape of today's society. This is because the concept of privacy has expanded in the face of advancing technologies. Innovations like artificial intelligence, quantum computing, and the Internet of Things have significantly shifted our traditional models of privacy, necessitating a reevaluation of our approaches to protecting and addressing online privacy (Agrawal, Gans and Goldfarb, 2019).

This section reviews the current political discourse on digital privacy and the regulatory framework of consent. We then examine prior research on the heuristics driving consumers' privacy decisions, particularly in the context of notice-and-choice. Finally, we describe the implications of privacy concerns on market competitiveness, innovation, and consumer welfare.

A. Notice-and-Choice Paradigm

Policymakers have traditionally considered consent, particularly notice-and-choice, as a conerstone of concept within the realm of digital privacy. In this paradigm, companies disclose the data they collect (the "notice"), and consumers choose whether to engage with the website (the "choice") (Turow et al., 2023). At the core of this framework are regulations such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), which mandate that businesses obtain informed user consent and ensure transparency in their data collection and usage practices.[2]. In addition to the GDPR and CCPA, new legislation continues to emerge in response to growing privacy concerns, prioritizing consent-based regulatory models Notable examples include Virginia's Consumer Data Protection Act (CDPA), the Colorado Privacy Act (CPA), and Sen. Roger Wicker's (R-Miss.) SAFE DATA Act[3]. Collectively,

[2]https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504; https://oag.ca.gov/privacy/ccpa

[3]Access to these bills can be found here, respectively: https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+HB2307ER

these regulations strive to empower consumers by providing greater control over the collection, usage, and protection of their personal data (Bleier, Goldfarb and Tucker, 2020).

However, while notice-and-choice mechanisms dominate political discourse, their effectiveness in today's digital economy is increasingly under question. These regulations are designed to protect consumers by placing the burden of decision-making on them, but this framework assumes that individuals can make rational trade-offs between privacy and other concerns (Stigler, 1980; Posner, 1981). What these consent-based regulations overlook, however, are the contextual and psychological factors that affect how consumers interact with privacy policies. Studies show that many individuals neither read nor understand the complex, legalistic privacy policies they are asked to accept, leading to what some scholars call the "privacy paradox" (Solove, 2012; Waldman, 2018; Richards and Hartzog, 2019; Nouwens et al., 2020). Furthermore, the cost of reading through privacy policies and understanding their implications is often too high for most consumers, placing an excessive burden on them (McDonald and Cranor, 2008). This reality raises serious concerns about whether current consent mechanisms are genuinely empowering consumers or simply shifting responsibility onto them without providing adequate tools or information to exercise their rights.

In this paper, we contribute to the ongoing debate by examining how firm characteristics such as size and legacy influence consumer behavior within consent-based privacy frameworks. Our findings have implications for if consumers are disproportionately swayed by subliminal factors like brand affinity, these consent mechanisms may unintentionally reinforce the dominance of large incumbent firms, further consolidating market power rather than fostering competition. As a result, our current reliance on notice-and-choice may not only fall short in empowering consumers but could also hinder innovation and harm consumer welfare.

B. The Mental Calculus of Privacy

Apart from the growing literature on notice-and-choice as a regulatory response, this project is related to the existing body of work in consumer psychology and decision-making. While consent frameworks are intended to promote competition and empower consumers, existing studies reveal that consumer decisions are

https://leg.colorado.gov/bills/sb21-190
https://www.congress.gov/bill/117th-congress/senate-bill/2499/text

often shaped by cognitive limitations, such as bounded rationality (Acquisti and Grossklags, 2005; Acquisti, Brandimarte and Loewenstein, 2015; Turow, Feldman and Meltzer, 2005) and hyperbolic discounting (Wang et al., 2011; Acquisti and Fong, 2020). These heuristics suggest that consumers do not approach privacy decisions as purely rational actors but are influenced by immediate concerns and mental shortcuts that can undermine their stated preferences for privacy. This disconnect is particularly evident in the "privacy paradox," where consumers express a desire for privacy but behave in ways that contradict those preferences in practice (Norberg, Horne and Horne, 2007; Athey, Catalini and Tucker, 2017). The implications of this paradox underscore how privacy regulations like consent-based models, may disproportionately impact small firms.

Moreover, Bleier, Goldfarb and Tucker (2020) that large incumbents are better equipped to absorb the costs of compliance, litigation, and potential revenue losses associated with privacy regulations, while smaller firms face greater challenges. Given that larger firms have greater access to capital and more robust networks, their ability to adapt to new regulations is less constrained, allowing them to absorb the costs of compliance with minimal disruption. In contrast, smaller firms, with fewer resources, may feel the impact of these regulatory changes more acutely, placing them at a competitive disadvantage. Aside from the mental shortcuts that consumers make when interacting with privacy policies, there is an existing body of work on the alternatives to address these decision shortcomings. For instance, privacy labels modeled after nutrition labels have been shown to improve the accuracy, speed, and satisfaction with which consumers engage with privacy information (Kelley et al., 2009).

In light of these findings, it becomes clear that consumer privacy decisions are shaped by both cognitive limitations and firm-specific factors where larger firms are better equipped to navigate the regulatory landscape. This body of literature demonstrates the disproportionate burden that consent-based privacy regulations place on smaller firms who are less positioned to handle the costs of compliance.

C. Economic Implications of Privacy Regulations

In addition to exploring how various factors influence online privacy behavior, our study examines the role that firm characteristics have on consumers' privacy preferences and its implications for market dynamics. A significant body of research has demonstrated that privacy regulations can shape market dynamics

in unintended ways. For example, Campbell, Goldfarb and Tucker (2015) presented a theoretical model illustrating that privacy regulations, while intended to protect consumers, may disproportionately favor large, incumbent firms over smaller entrants, especially in targeted advertising markets. Further complicating this dynamic, Jia, Jin and Wagman (2021) found that post-GDPR, there were disproportionately adverse effects on venture capital investment into technology firms. Similarly, Johnson, Shriver and Goldberg (2023) identified a significant increase in market concentration among web technology vendors following GDPR's compliance deadline, with EU residents experiencing a 15% reduction in website use of smaller technology vendors and a 17% rise in vendor market concentration. These results indicate the potential for privacy regulation to exacerbate monopolistic tendencies by creating barriers for smaller firms.

Moreover, the broader economic effects of privacy regulations extend beyond competition and innovation. Studies have shown that privacy regulation can slow technology diffusion (Miller and Tucker, 2009), increase data breaches Miller and Tucker (2011), and reduce web traffic and revenue (Schmitt, Miller and Skiera, 2022; Bleier, Goldfarb and Tucker, 2020; Goldberg, Johnson and Shriver, 2024). These adverse effects suggest that privacy regulations, while well-intentioned, may have far-reaching consequences that are not fully accounted for in their design.

Our study builds on this body of work by examining how firm characteristics interact with regulatory dynamics to shape consumers' privacy decisions. However, unlike prior work that has primarily focused on the use of dark patterns in privacy policies or the impact of privacy regulations on firm performance, our experimental approach isolates the role of firm-specific factors, such as size and legacy, in shaping consumer behavior. In doing so, we provide new insights into the potential cascading effects of privacy regulations on market dynamics, contributing to the broader conversation on how to design privacy regulations that promote both consumer protection and healthy competition.

II. Method

A. Overview

We conducted a between-subjects online experiment to investigate consumers' behavior in response to cookie consent requests. Data was collected through CloudResearch (formerly TurkPrime), a third-party platform facilitating online

participant recruitment. The study consisted of two main components: (1) an online experiment examining how company characteristics influence consumers' willingness to accept cookies; and (2) a post-experiment survey assessing attitudes towards privacy regulations and factors impacting cookie consent behavior.

B. Experimental Design

Participants were introduced to a fictitious company, *Zenith Computing*, and were asked to interact with its cookie consent screen. We intentionally chose the name Zenith Computing to avoid associations with well-known technology companies, minimizing potential bias in participants' responses. The website featured common elements of a corporate tech site, such as tabs for 'About Us,' 'Our Services,' and 'Careers'. The cookie consent banner, inspired by industry-standard designs, provided clear information on data collection for security, functionality, and targeted advertising, and presented participants with the option to 'Accept' or 'Decline' cookies (see Figure 1). The website and interface were consistent across all experimental conditions, ensuring that only the independent variables—firm size, legacy, and product mix—varied. This design allowed us to isolate the effects of these variables on participants' willingness to accept cookies, without interference from other confounding factors.

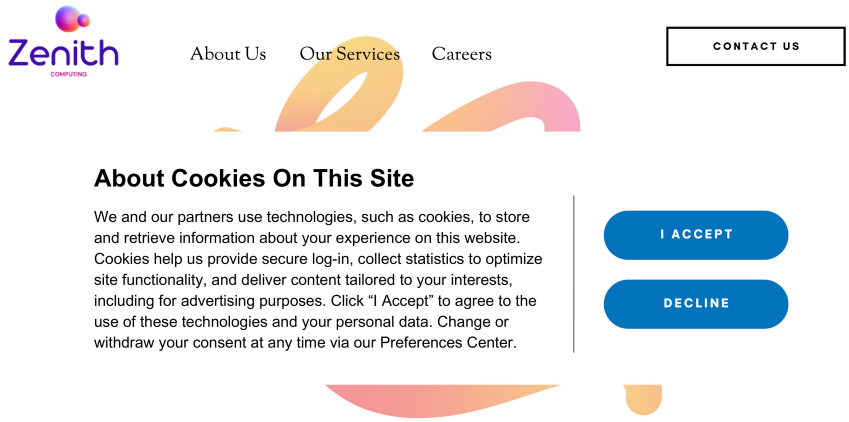

Figure 1. Zenith Computing's cookie consent banner

The study used a between-subjects design with four conditions, each defined by three binary factors: firm size, legacy, and product mix. We defined *size* as either a small firm with 100 employees or a large firm with 25,000 employees. *Legacy* was categorized based on the firm's age—either a newer company with less than five years in business or an established firm with 25 years of experience. Lastly, firms were classified by *product mix*, with some selling physical products such as phones, headphones, and watches, while others derived revenue primarily from digital advertising. Participants were randomly assigned to one of the following four experimental conditions:

1) Large-legacy-digital: Large firm with 25,000 employees, established for 25 years, operating with a digital advertising business model.

2) Large-legacy-hardware: Large firm with 25,000 employees, established for 25 years, operating with a hardware and physical products business model.

3) Large-new-digital: Large firm with 25,000 employees, established for less than 4 years, operating with a digital advertising business model.

4) Small-legacy-digital: Small firm with 100 employees, established for 25 years, operating with a digital advertising business model.

We chose these four conditions out of the possible eight other combinations because they allowed us to isolate one dimension. The first condition, defined by large size, established legacy, and a digital advertising model, served as the main treatment group. The other three conditions change in only one aspect relative to the first condition. This allowed us to hold other potential confounding factors constant and isolate any causal relationships between these different dimensions and our primary dependent variable.

C. Hypotheses

Drawing on established economic and psychological theories, we develop the following hypotheses to explain consumer behavior in privacy-related decisions, particularly in the context of the General Data Protection Regulation (GDPR) and notice-and-choice consent mechanisms. Our primary hypothesis is rooted in *Signaling Theory* (Spence, 1973), which posits that firm characteristics, such

as size, function as indicators of reliability and competence. Thus, we argue that large firms, due to their established market presence, extensive resources, and longevity in the market, are more likely to be perceived by consumers as trustworthy and reliable stewards of sensitive data. The legacy of large firms reinforces a perception of stability, signaling to consumers that these firms have reliably complied with regulatory obligations, thereby placing trust in their data management practices.

We also build upon the *Resource-Based View* (Barney, 1991), which asserts that firms maintain competitive advantage by leveraging valuable, rare, inimitable, and non-substitutable resources. In the context of data privacy, larger firms can more effectively utilize data as a strategic resource, enhancing their market dominance through heightened consumer trust and perceived legitimacy. Their scale and infrastructure allow them to implement advanced security measures and compliance mechanisms, which consumers may interpret as superior to those of smaller firms. Consequently, privacy concerns may unintentionally reinforce the competitive positions of incumbents, exacerbating disparities between large firms and smaller competitors. Based on this theoretical framework, we propose the following hypothesis:

Hypothesis: *Consumers will exhibit a significantly lower willingness to accept data-tracking consent to small start-up firms compared to large incumbent firms.*

D. Participants and Procedure

A total of 153 participants successfully finished both the experiment and survey (Mage = 42.4, SD = 14.9; 44.1% female). Refer to table 1 for a more detailed overview of partipants. We recruited participants through CloudResearch. They were compensated $1 for the completion of the survey. All participants resided in the United States during the time of this study. We removed 52 responses using attention-check questions for a total sample of 101.

Participants were notified and given an informed consent page before proceeding with the study. After reading and agreeing to participate in the study, participants were randomly assigned and given a short description of Zenith Computing according to one of the four experimental conditions described above. On the same screen, all participants were shown a simulated interface of Zenith Com-

Table 1—Summary Statistics of Survey Respondents

Demographic Variables	Frequency (%)
Gender	
Male	66 (43.14%)
Female	84 (54.90%)
Other/Prefer not to say	3 (1.96%)
Political Affiliation	
Liberal/Very Liberal	52 (33.99%)
Conservative/Very Conservative	43 (28.10%)
Moderate/No Preference	58 (37.91%)
Education	
High School or less	45 (29.41%)
Some College/Trade School	11 (7.19%)
Bachelor's Degree	59 (38.56%)
Master's Degree or higher	35 (22.88%)
Prefer not to say	3 (1.96%)
Annual Household Income	
$0-$49,999	61 (39.87%)
$50,000-$99,999	54 (35.29%)
$100,000-$149,999	22 (14.38%)
$150,000 or more	9 (5.88%)
Prefer not to say	7 (4.58%)

puting's homepage with a cookie consent banner shown in Figure 1. Once read, the participants were asked on a seven-point Likert scale how much they agreed to the statement that they would click 'I accept' cookies, considering the information provided about the company. This was our primary dependent variable. Immediately after answering this question, participants were asked a series of similar questions around comfortability and trust with Zenith Computing using cookies. These questions were used as a composite measure and based on a seven-point Likert scale with endpoints "strongly disagree" and "strongly agree." This concluded the first section of our survey experiment (i.e., the experiment).

We partitioned the following sections of our survey into three parts: section 2 asked a number of questions about familiarity with and opinions about existing and proposed regulations related to privacy; section 3 asked participants about typical habits surrounding their privacy preferences and technology use; and finally section 4 asked a series of standard demographic questions. After completing both the experiment and survey, the participants were given the completion code

that was required in order to confirm the completion of the survey and receive their compensation. The completion time for the experiment and survey was less than three days.

III. Results

A. Experimental results.

In our experiment, participants were asked to rate their likelihood of clicking "I accept" on Zenith Computing's cookie consent request using a seven-point Likert scale, ranging from "strongly disagree" to "strongly agree." Upon comparing the average Likert scores across the experimental conditions, no statistically significant differences were found between the primary treatment group (large, established firms) and the other three conditions. However, it is important to acknowledge the limited sample sizes within these groups, which may have impacted the statistical power of the analysis. Table 2 presents a summary of the t-test results.

Table 2—Experimental Results by Stimulus

Stimulus	Test Statistic	p-value	Difference	95% Lower Bound	N
Large-old-products	0.05	0.479	0.033	(-1.03)	24
Large-new-ads	0.24	0.407	0.171	(-1.04)	17
Small-old-ads	1.12	0.135	0.625	(-0.317)	40

Although the results are not statistically significant, the directional trends observed in this experiment offer valuable insights into how consumers perceive privacy and consent across different brand conditions (Figure 3). The highest average Likert score (4.70), associated with large, established brands, suggests that consumers are generally more comfortable accepting data tracking from well-known, long-standing companies. This is consistent with the hypothesis that larger firms are seen as more trustworthy due to their market presence and perceived reliability. The minimal change in the Likert score when the product dimension shifts from advertising to physical products (4.70 to 4.67) indicates that the type of offering, whether abstract (ads) or tangible (products), has little influence on consumer decisions regarding cookie consent. This suggests that brand perception, rather than the nature of the product, may play a larger role in shaping

privacy-related decisions.

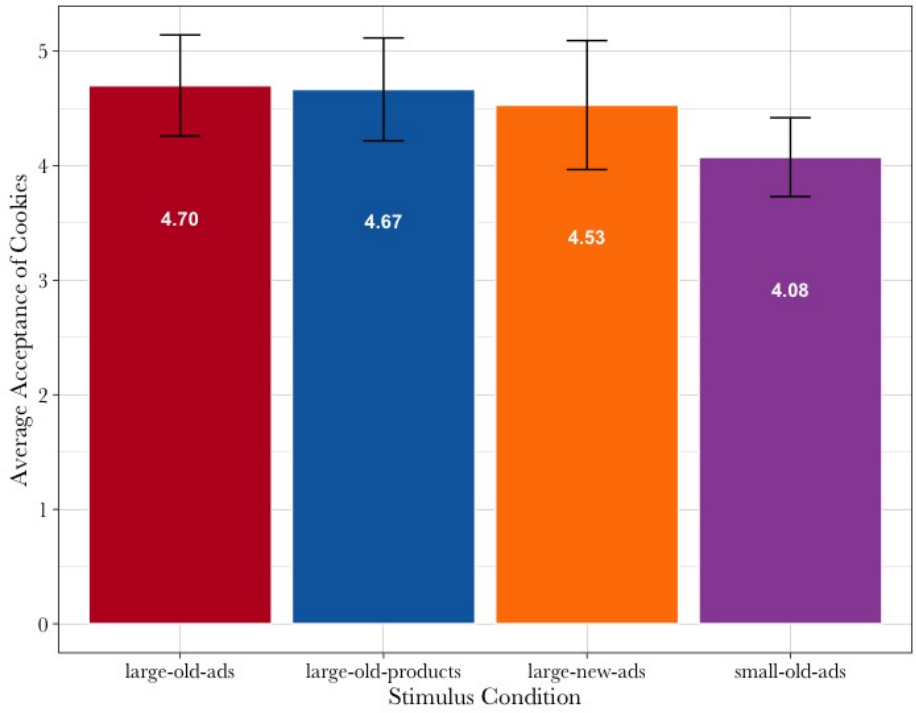

Figure 2. Difference in Average Likert Response Across Stimuli

A more meaningful shift occurs when the brand legacy changes from old to new (4.70 to 4.53), implying that a brand's longevity has a measurable impact on consumer trust. Newer companies, regardless of size, may be perceived as less reliable in handling personal data, reflecting consumers' tendency to trust established firms over newcomers, likely due to familiarity or reputation. The most notable result comes from the comparison between small, established brands and the main treatment group, which highlights a significant decrease in consumers' willingness to accept cookies. This suggests that consumers may not simply equate size with trustworthiness; rather, a brand's legacy and reputation also significantly affect their comfort with data sharing. The gap between these conditions emphasizes that while larger, well-known firms benefit from consumer trust, smaller brands—even those with an established presence—may face challenges in convincing consumers to consent to data tracking.

While not statistically significant, these results reveal important directional trends in how consumers make privacy decisions based on firm characteristics. Consumers appear to place less emphasis on a brand's product mix but are more influenced by factors such as brand legacy and size. The observed heterogeneity in privacy choices suggests that firm attributes play a key role in data-tracking consent decisions. Future research with larger sample sizes is needed to confirm these trends and provide a more definitive understanding of their impact.

B. Survey results

Differences in trust. In our survey, participants rated their agreement with the statement, "I trust this company to use and store my personal data responsibly and in a manner that I would find acceptable," using a seven-point Likert scale across 14 different organization types. These organization types included a mix of companies such as Apple, personal hospitals, and nonprofits, representing a range of industries and public trust levels. The analysis revealed a significant difference in trust between two specific types of organizations: (1) a large, established company with over 25 years of experience, and (2) a newly emerged start-up with fewer than 100 employees (Figure 3). This contrast highlights the impact of both company size and brand legacy on consumer trust in data privacy practices.

The average trust reported for large firms was significantly higher than for small start-ups (d = 1.14, p ¡ 0.01, 95% CI: 0.74, inf). This supports our hypothesis that consumers tend to trust large, well-established firms more than smaller, newer ones. These results suggest that firm size and longevity play a key role in consumer perceptions of data security and responsibility. Larger firms, with decades of experience, may benefit from an established reputation and brand familiarity, factors that can enhance consumer trust, even if the firm's actual privacy practices are unknown. In contrast, smaller start-ups, which lack this legacy and public familiarity, may be perceived as riskier when it comes to handling sensitive personal data.

Although the results do not imply causality, they offer strong evidence that consumers are inclined to trust larger, more established companies—possibly due to an assumption that these firms have more resources, better security infrastructure, and more at stake in maintaining their reputations. This trust disparity may create competitive advantages for large incumbents, as they can leverage their perceived reliability to attract more users, potentially widening the gap

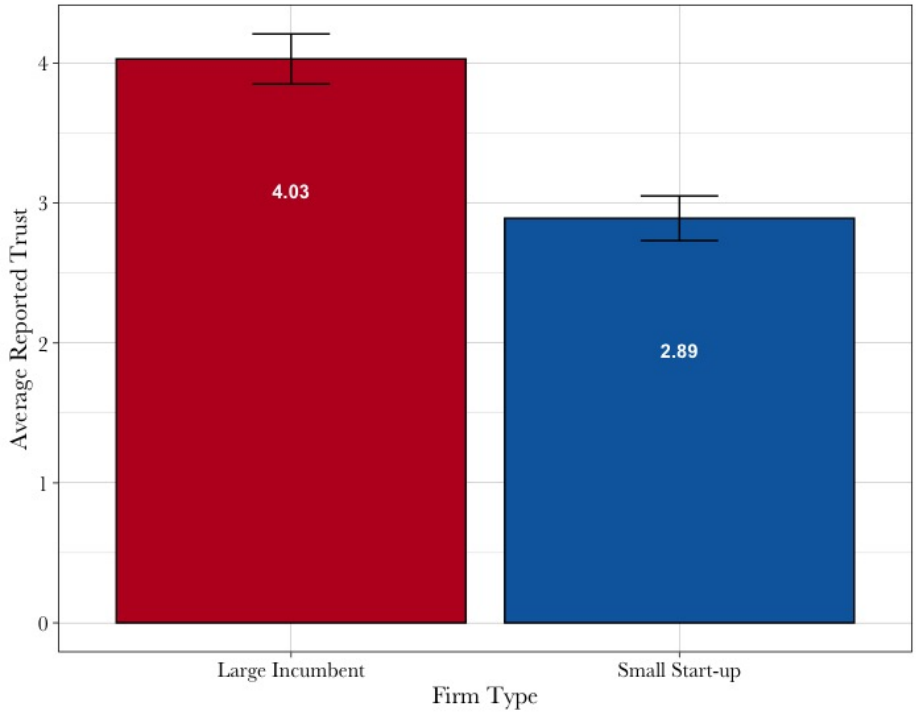

Figure 3. Average Reported Difference in Trust Across Large and Small Firms

between themselves and smaller competitors. Furthermore, the findings suggest that newer, smaller firms may face an uphill battle in earning consumer trust, despite possibly offering superior privacy practices.

General awareness of privacy regulation. When participants were asked about their general awareness of privacy regulations like the GDPR and CCPA, nearly a third reported being "not at all aware" (Table 3). Fewer than 10% indicated they were "moderately aware" or "extremely aware." Additionally, many respondents mentioned that they typically agree to cookie policies in less than 10 seconds, despite encountering them more than once per day. These findings highlight a significant gap between the intent behind privacy regulations and the public's actual awareness and engagement with them.

This low level of awareness suggests that privacy laws, although designed to protect consumers, may not be having their intended effect if individuals are unaware of their rights or do not take the time to fully understand the policies they are agreeing to. The fact that many users consent so quickly to cookie policies

Table 3—Awareness by Regulation

Response	GDPR Proportion	CCPA Proportion
Not at all aware	0.57	0.52
Somewhat aware	0.13	0.08
Moderately aware	0.12	0.13
Slightly aware	0.12	0.21
Extremely aware	0.07	0.07
Total	101	101

underscores a behavior of convenience, rather than informed decision-making. This disconnect between policy and practice points to a need for better education and communication strategies around privacy regulations to help consumers make more informed choices regarding their personal data. Moreover, it suggests that regulators may need to rethink how consent mechanisms are designed, as quick acceptance without understanding undermines the very purpose of these regulations.

C. General Discussion

Our results suggest that regulating privacy is much more complex than simply adopting consent mechanisms like notice and choice. While regulators endeavor to promote competition and empower consumers, our study demonstrates that these two goals do not work in tandem. Although our experimental evidence is not significant, there are directional effects showing that consumers evaluate their privacy options and decisions differently depending on a firm's characteristics. Most prominent is the difference for small firms. This is further shown in our survey evidence, where participants trusted and thus favored large incumbent firms over their smaller counterparts. Though this does not imply a causal relationship, it demonstrates that subtle factors like a brand's size, legacy, or even industry can influence the proportion of cookie acceptance.

Policymakers should be aware that certain well-intended regulations might have undesired downstream effects. For instance, if consumers favor larger firms regarding their privacy requests compared to others, such preferences can exacerbate competition, leading to further market consolidation and affecting market dynamics. Behind the backdrop of these privacy decision-making processes is the

fact that consumers are predominantly unaware of existing privacy regulations. As consumers remain largely uninformed about their rights and data protection measures, it becomes imperative for policymakers to bridge this knowledge gap and strengthen privacy literacy among the public.

D. Limitations

One of the main limitations of this study is the small sample, which consisted of 101 participants. The limited sample may explain the difficulty of finding a significant relationship in our experiment. Even though we attempted to garner a representative sample through CloudResearch, our insufficient sample may have restricted the statistical power and generalizability of the findings. Future research should employ a larger sample size to enhance the statistical power and improve the generalizability of the findings.

Although we included attention-check questions and removed responses that responded incorrectly, our survey was relatively lengthy. The extended length of our survey could lead to survey fatigue, in which respondents may have become fatigued or disengaged, possibly affecting the accuracy and reliability of their responses. This survey fatigue may have contributed to rushed or less thoughtful answers.

IV. Conclusion

The goals of this project have been to provide insight into the implications of consent-based privacy regulations. We conducted a two-part study, finding that the characteristic of firms can have an impact on consumers' privacy decision-making. We first conducted a between-subject experiment asking participants about their willingness to accept cookies under one of four conditions. Despite insignificant results, we found directional effects showing that consumers differentially evaluated their privacy choices based on a brand's legacy, size, and product mix. Our post-experiment survey reinforces these observations. When asked to rate their trust in different organizations, respondents indicated lower average trust in small start-ups than in large incumbent firms. These findings provide both meaningful insights and contribute to the broader literature on digital privacy. We have shown that consumers are largely unaware of privacy regulations, and when they do interact with cookie banners enforced by these regulations, it is often impacted by subliminal factors.

While regulations like the GDPR and CCPA should be lauded for striving to encourage competition and empower consumers, these regulations may inadvertently reduce competition and leave consumers worse off. In other words, these policies that strive to improve the welfare of the general public may end up reducing it through more giant monopolies, increased prices, and fewer options. Therefore, policymakers have to be cautious with solely subscribing to the notice and choice paradigm for privacy regulations since it may reduce competition and cause more harm than good.

Though there is room for future work in this area, this research represents an important contribution to our understanding of the subtle factors that may impact consumers' privacy choices. By illustrating the variation of privacy evaluations individuals have based on different firm characteristics, we have provided meaningful insight into how consumers evaluate their privacy policies and the potential implications of these decisions on competition. We hope future research can build on this project to further our approaches to promoting competition and empowering consumers through effective online privacy regulations.

REFERENCES

Aaker, David. 1991. "Brand equity." *La gestione del valore della marca*, 347: 356.

Acquisti, Alessandro, and Christina Fong. 2020. "An experiment in hiring discrimination via online social networks." *Management Science*, 66(3): 1005–1024.

Acquisti, Alessandro, and Jens Grossklags. 2005. "Privacy and rationality in individual decision making." *IEEE security & privacy*, 3(1): 26–33.

Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. 2015. "Privacy and human behavior in the age of information." *Science*, 347(6221): 509–514.

Acquisti, Alessandro, Leslie K John, and George Loewenstein. 2013. "What is privacy worth?" *The Journal of Legal Studies*, 42(2): 249–274.

Agrawal, Ajay, Joshua S Gans, and Avi Goldfarb. 2019. "Exploring the impact of artificial intelligence: Prediction versus judgment." *Information Economics and Policy*, 47: 1–6.

Aridor, Guy, Yeon-Koo Che, and Tobias Salz. 2021. "The effect of privacy regulation on the data industry: Empirical evidence from GDPR." 93–94.

Athey, Susan, Christian Catalini, and Catherine Tucker. 2017. "The digital privacy paradox: Small money, small costs, small talk." National Bureau of Economic Research.

Barney, Jay. 1991. "Firm resources and sustained competitive advantage." *Journal of management*, 17(1): 99–120.

Bleier, Alexander, Avi Goldfarb, and Catherine Tucker. 2020. "Consumer privacy and the future of data-based innovation and marketing." *International Journal of Research in Marketing*, 37(3): 466–480.

Bonatti, Alessandro. 2022. "The Platform Dimension of Digital Privacy." National Bureau of Economic Research.

Brough, Aaron R, David A Norton, Shannon L Sciarappa, and Leslie K John. 2022. "The bulletproof glass effect: Unintended consequences of privacy notices." *Journal of Marketing Research*, 59(4): 739–754.

Brynjolfsson, Erik, and Brian Kahin. 2002. *Understanding the digital economy: data, tools, and research.* MIT press.

Campbell, James, Avi Goldfarb, and Catherine Tucker. 2015. "Privacy regulation and market structure." *Journal of Economics & Management Strategy*, 24(1): 47–73.

Chellappa, Ramnath K, and Raymond G Sin. 2005. "Personalization versus privacy: An empirical examination of the online consumer's dilemma." *Information technology and management*, 6: 181–202.

Collis, Avinash, Alex Moehring, Ananya Sen, and Alessandro Acquisti. 2021. "Information frictions and heterogeneity in valuations of personal data." *Available at SSRN 3974826*.

Goldberg, Samuel G, Garrett A Johnson, and Scott K Shriver. 2024. "Regulating privacy online: An economic evaluation of the GDPR." *American Economic Journal: Economic Policy*, 16(1): 325–358.

Goldfarb, Avi, and Catherine Tucker. 2012. "Shifts in privacy concerns." *American Economic Review*, 102(3): 349–353.

Goldfarb, Avi, and Catherine Tucker. 2019. "Digital economics." *Journal of economic literature*, 57(1): 3–43.

Hong, Weiyin, Frank KY Chan, and James YL Thong. 2021. "Drivers and inhibitors of internet privacy concern: a multidimensional development theory perspective." *Journal of Business Ethics*, 168: 539–564.

Jia, Jian, Ginger Zhe Jin, and Liad Wagman. 2021. "The short-run effects of the general data protection regulation on technology venture investment." *Marketing Science*, 40(4): 661–684.

Johnson, Garrett A, Scott K Shriver, and Samuel G Goldberg. 2023. "Privacy and market concentration: intended and unintended consequences of the GDPR." *Management Science*.

Kelley, Patrick Gage, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. "A "nutrition label" for privacy." *SOUPS '09*. New York, NY, USA:Association for Computing Machinery.

Kim, Dongyeon, Kyuhong Park, Yongjin Park, and Jae-Hyeon Ahn. 2019. "Willingness to provide personal information: Perspective of privacy calculus in IoT services." *Computers in Human Behavior*, 92: 273–281.

Kosta, Eleni. 2020. "345 Article 7 Conditions for consent." In *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press.

Marchant, Gary E. 2011. *The growing gap between emerging technologies and the law.* Springer.

McDonald, Aleecia M, and Lorrie Faith Cranor. 2008. "The cost of reading privacy policies." *Isjlp*, 4: 543.

Miller, Amalia R, and Catherine E Tucker. 2011. "Can health care information technology save babies?" *Journal of Political Economy*, 119(2): 289–324.

Miller, Amalia R, and Catherine Tucker. 2009. "Privacy protection and technology diffusion: The case of electronic medical records." *Management science*, 55(7): 1077–1093.

Norberg, Patricia A, Daniel R Horne, and David A Horne. 2007. "The privacy paradox: Personal information disclosure intentions versus behaviors." *Journal of consumer affairs*, 41(1): 100–126.

Nouwens, Midas, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. "Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence." 1–13.

Posner, Richard A. 1981. "The economics of privacy." *The American economic review*, 71(2): 405–409.

Richards, Neil, and Woodrow Hartzog. 2019. "Taking Trust Seriously in Privacy Law'(2016)." *Stanford Technology Law Review*, 19: 431.

Schmitt, Julia, Klaus M Miller, and Bernd Skiera. 2022. "The impact of privacy laws on online user behavior." *HEC Paris Research Paper*.

Solove, Daniel J. 2012. "Introduction: Privacy self-management and the consent dilemma." *Harv. L. Rev.*, 126: 1880.

Spence, Michael. 1973. "Job market signaling." *The quarterly journal of Economics*, 87(3): 355–374.

Stigler, George J. 1980. "An introduction to privacy in economics and politics." *The Journal of Legal Studies*, 9(4): 623–644.

Turow, Joseph, Lauren Feldman, and Kimberly Meltzer. 2005. "Open to exploitation: America's shoppers online and offline." *Departmental Papers (ASC)*, 35.

Turow, Joseph, Yphtach Lelkes, Nora Draper, and Ari Ezra Waldman. 2023. "Americans Can't Consent to Companies' Use of Their Data: They Admit They Don't Understand It, Say They're Helpless to Control It, and Believe They're Harmed When Firms Use Their Data–Making What Companies Do Illegitimate." *Say They're Helpless to Control It, and Believe They're Harmed When Firms Use Their Data–Making What Companies Do Illegitimate (February 15, 2023)*.

Urde, Mats, Stephen A Greyser, and John MT Balmer. 2007. "Corporate brands with a heritage." *Journal of Brand Management*, 15: 4–19.

Utz, Christine, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. "(Un) informed consent: Studying GDPR consent notices in the field." 973–990.

Waldman, Ari Ezra. 2018. "Privacy, notice, and design." *Stan. Tech. L. Rev.*, 21: 74.

Wang, Yang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. 2011. "" I regretted the minute I pressed share" a qualitative study of regrets on Facebook." 1–16.

Warren, Samuel D, and Louis D Brandeis. 1890. "The right to privacy." *Harvard Law Review*, 4(5): 193–220.

Wharton. 2019. "Data as Currency: How Advertising Works Today."