Privacy Lost? Consumer Digital Privacy and Earnings Benchmarks*

Wen-Hsin (Molly) Chang
UCLA Anderson School of Management

April 26, 2025

*I am grateful for all the helpful comments from Judson Caskey, Carla Hayn, Henry Friedman, and Mark Kim. All errors are my own.

Privacy Lost? Consumer Digital Privacy and Earnings Benchmarks

Abstract

This study examines whether earnings benchmarks influence firms' aggressiveness toward consumer digital privacy. I find that firms narrowly beating the prior year's earnings engage in significantly higher third-party online tracking within their domains, even after controlling for conventional accrual-based and real activity-based earnings management (EM) channels. Two mechanisms explain these findings: increased tracking boosts site visits via personalized ads and enhances discretionary spending effectiveness. However, using the Sustainability Accounting Standards Board (SASB) materiality indicator to assess the overall costs of consumer privacy, I find that the main effect weakens when consumer privacy poses a material sustainability risk or when firms assign a board committee to oversee data governance. Overall, this research highlights firms' responses to earnings benchmarks in the increasingly important yet often hidden digital space, affecting almost everyone via the Internet.

Keywords: Digital Privacy; Earnings Benchmarks; Materiality; Data Governance; Technology

JEL classification: M14; M43; O33

1 Introduction

In the digital era, consumer data holds substantial commercial value, as it enables firms to "read the minds" of consumers and drives advancements in technologies such as business analytics and artificial intelligence (AI). However, as firms increasingly rely on data-driven decision-making, concerns about digital privacy also arise. For example, in 2024, PayPal revised its privacy policies to expand the collection and sharing of consumer data with third-party marketers.[1] As both the benefits and costs increase with the amount of consumer data collected, this study examines whether earnings benchmarks influence firms' aggressiveness toward consumer digital privacy, after controlling for traditional accrual-based and real activity-based earnings management (EM) channels. The research question is highly relevant to accounting as it highlights the evolution of EM channels over time, from traditional accrual-based methods to real activities emerging in the digital space.

While the Business Application Research Center (BARC) finds that data analytics increases revenue by 8 percent and reduces costs by 10 percent, a survey by KPMG reveals that 68 percent of US adults are concerned about how much data businesses collect.[2] Concerns about digital privacy prompt firms to continually modify their data strategies to meet evolving needs and comply with regulatory requirements (e.g., Johnson et al. 2023; Lefrere et al. 2022; Abraham et al. 2019). A key development is the "right to be forgotten," established by the European Court of Justice in a 2014 case against Google and later codified in the General Data Protection Regulation (GDPR).[3] The Sustainability Accounting Standards Board (SASB) also identifies consumer privacy as a material sustainability risk that may affect firms' current or future cash flows. In recent years, more firms have emphasized

[1] Available at: https://www.wsj.com/personal-finance/paypal-sell-customer-purchase-data-266b0e79

[2] Available at https://bi-survey.com/big-data-benefits, and https://kpmg.com/us/en/articles/2023/bridging-the-trust-chasm.html

[3] The right to be forgotten primarily imposes an obligation on data processors to promptly erase personal data when it is no longer required for its original purpose.

data governance in their SEC filings and have assigned board committees, such as audit committees, to oversee consumer privacy concerns. (e.g., Klein et al. 2022).[4]

This study measures a firm's aggressiveness toward consumer digital privacy based on the intensity of third-party tracking within its domain. To account for variations by industry, website purpose, and year trends, I measure abnormal third-party tracking as the deviation from the industry, year, and site category averages. Third-party trackers are scripts, codes, or pixels embedded on a firm's website that collect and share visitor data with external entities. For example, in September 2024, macys.com had an average of 14 third-party trackers per page load according to Whotracks.me, with the main categories spanning advertising, site analytics, and customer interactions (see Appendix B for examples of third-party trackers).[5] Third-party trackers lead to privacy concerns because site visitors are often "notified but unaware" of the extent of data collection and sharing (Larsson et al. 2021). Additionally, third-party trackers often collect visitors' online activities across multiple websites and share the information within an ecosystem of advertising networks, data brokers, and credit rating agencies, leading to unexpected uses of personal information.[6]

The tests measure trackers relative to the industry-site category-year mean, hereafter "abnormal tracking." Using a difference-in-differences design, I show that US sites exhibit significantly lower abnormal tracking intensity than Canadian sites after the milestone California Consumer Privacy Act (CCPA) took effect in January 2020. The findings validate the abnormal tracking measure as an indicator of firms' aggressiveness toward consumer digital privacy. Abnormal tracking is negatively associated with abnormal accruals and ab-

[4]Firms' data governance practices extend beyond regulatory compliance. For example, The RealReal, Inc.'s 2021 proxy statement mentioned, "there is a cost and risk associated with every piece of data our customers entrust us with, so we take measures to minimize what is collected." Similarly, ServiceNow, Inc.'s 2021 proxy statement mentioned they "consider data use cases which, although legally permitted, may not meet their standards for maintaining customers' trust."

[5]Available at: https://www.ghostery.com/whotracksme/websites/macys.com

[6]See Mayer and Mitchell (2012) for a detailed explanation of third-party web tracking. A detailed illustration is also available at: https://www.eff.org/wp/behind-the-one-way-mirror

normal production. In contrast, it is positively and significantly associated with abnormal cuts in discretionary spending, suggesting that firms intensify online tracking as a complement to remaining discretionary activities, including advertising, research and development (R&D), and selling, general, and administrative (SG&A).

This study focuses on avoiding annual earnings decreases as a crucial benchmark, as maintaining a positive earnings string is often emphasized in the media (e.g., Burgstahler and Dichev 1997; Myers et al. 2007; Barth et al. 1999). I find that firms narrowly beating the previous year's earnings engage in abnormally high third-party online tracking within their domains, even after controlling for conventional accrual-based and real activity-based earnings management channels. The increase in trackers represents approximately 20 percent of mean tracker usage in the sample.[7] On average, the sample shows an increase in tracking intensity two months before the annual fiscal year-end. Online tracking is expected to sustain earnings growth by monitoring changes in consumer behavior in real-time. These results remain robust when using analysts' consensus annual EPS forecasts as the earnings benchmark.[8] I show two mechanisms underlying the findings: intensified tracking (1) boosts site visits through personalized advertising and expanded advertising networks, and (2) enhances the efficiency of discretionary spending. These mechanisms align with previous research indicating that third-party trackers are frequently utilized for advertising and site analytics purposes (e.g., Karaj et al. 2018).

Moreover, I explore two additional hypotheses that consider (1) the materiality of consumer privacy and (2) board committee privacy oversight. First, the SASB's classification

[7]I interpret the results as firms making decisions with long-term ramifications to meet short-term benchmarks. Approximately 19 percent of the suspect firms in my sample exhibit lower tracking intensity in the following year, similar to Vorst (2016) which shows only 18.3 (9.2) percent of firms subsequently reverse the R&D (SG&A) cuts.

[8]The test using analysts' consensus annual forecasts as a benchmark yields a smaller economic magnitude. The primary distinction of analysts' forecasts is that they serve as a moving benchmark, in contrast to the static nature of the previous year's earnings.

of consumer privacy as a sustainability risk summarizes both the direct (e.g., regulatory and litigation risks) and indirect (e.g., loss of customer trust) costs of abnormal tracking, serving as a useful summary statistic for consumer privacy costs. I find that the relation between abnormal tracking and earnings benchmarks is less pronounced for firms in industries where consumer privacy is a material sustainability risk. Second, to further address the alternative explanation that abnormally high tracking reflects a firm's operating environment rather than incentives to avoid missing earnings benchmarks, I examine cases where a firm publicly designates a board committee to oversee data practices. Failure to adhere to these practices could lead to misleading public statements and potential litigation.[9] I find that the association between abnormal tracking and earnings benchmarks is less pronounced for firms with consumer privacy explicitly delegated to specific board committees, as indicated in their DEF14A proxy statements. If intensified tracking is an optimal response, it becomes difficult to explain why a firm's own privacy oversight and materiality would limit such customer tracking tendencies. Taken together, the two cross-sectional results address why not all firms track their visitors as extensively as possible.

This study contributes to the literature in three ways. First, it adds to the literature on firms' responses to earnings benchmarks. Managers have incentives to sacrifice long-term value to avoid missing earnings benchmarks by manipulating accruals or real activities, such as reducing discretionary expenses, overproduction, or temporary sales discounts (e.g., Dechow et al. 1995; Roychowdhury 2006). Recent studies have examined issues such as employee safety and emissions (Caskey and Ozel 2017; Liu et al. 2021). In contrast to prior studies, this paper explores an increasingly important yet often overlooked area: the digital space, uncovering a hidden mechanism that firms exploit to meet annual earnings

[9] For examples of securities class action complaints related to misleading disclosures of firms' consumer online privacy practices, see Complaint, Gordon v. Nielsen Holdings Plc, No. 18-cv-07143 (S.D.N.Y. August 8, 2018), and Complaint, Monsky v. Digital Holdings, Inc., No. 24-cv-01940 (S.D. Tex. May 23, 2024).

benchmarks at the expense of consumer digital privacy. I also enrich the EM literature by exploring EM strategies in the digital economy. For example, the overproduction earnings management channel may be less relevant for digital platforms, while accrual-based channels may be less applicable to firms with minimal accruals due to direct revenue recognition, prior balance sheet overstatements (e.g., Barton and Simko 2002), or a higher risk of prosecution.

In addition, the study contributes to the literature on the determinants of firms' data strategies, especially regarding data collection and sharing. Previous marketing research shows that regulations, such as the GDPR, are followed by a short-term drop in third-party online trackers, often those of lower quality, to ensure regulatory compliance (e.g., Peukert et al. 2022; Johnson et al. 2023; Lefrere et al. 2022). I document a financial reporting incentive that prompts aggressive consumer privacy practices- when firms are at risk of missing annual earnings benchmarks. This study also highlights the mitigating effects of board committees' privacy oversight and materiality considerations.

Finally, this study extends the emerging accounting literature on data privacy breaches by viewing firms as potential perpetrators of consumer privacy rather than victims lacking adequate controls. While several accounting studies have focused on cybersecurity (e.g., Ashraf and Sunder 2023; Ashraf 2022; Huang and Wang 2021; Amir et al. 2018), there is relatively less emphasis on consumer digital privacy.[10] It is crucial to study digital privacy and cybersecurity separately, as each has different implications. For example, firms that fall victim to external cyberattacks may receive insurance compensation, and the public may perceive the breach less negatively if firms respond promptly (e.g., Richardson et al.

[10] For further reading on recent cybersecurity research from management and accounting perspectives, see Lohrke and Frownfelter-Lohrke (2023) and Haapamäki and Sihvonen (2019). Some studies, such as Klein et al. (2022), have used the term "cyber risk" to encompass the overall risks associated with cybersecurity, cyberattacks, and data privacy. These studies typically use firms' self-reported or governmental records of data breaches from the Audit Analytics cybersecurity database or Privacy Rights Clearinghouse for their inferences.

2019).[11] However, in cases where firms are perpetrators of digital privacy violations, they assume the primary responsibility.

2 Background

2.1 Public enforcement for consumer digital privacy

Firms' incentives to safeguard consumer digital privacy are driven by heightened privacy-related risk exposures, particularly public and private enforcement. These privacy-related risks are exacerbated by increased data collection and third-party involvement through intensified online tracking. Regulatory risks include fines for privacy noncompliance. For example, the General Data Protection Regulation (GDPR), which took effect in May 2018, is a landmark law aimed at ensuring the privacy of European Union (EU) citizens and applies to many US firms that serve at least one EU user. Penalties for GDPR violations can amount to the higher of 20 million euros or 4 percent of a firm's annual revenue from the prior year (Article 83). The GDPR protects users' data rights and imposes obligations on firms, including the requirement to establish a legal basis for data processing, such as obtaining explicit consent and processing personal data only when necessary.[12] Notably, the GDPR holds companies jointly accountable for third-party violations, making it necessary for firms to ensure third-party compliance (Article 28(1)).[13]

In recent years, U.S. privacy regulations have seen significant advancements. The Cal-

[11] In the 2013 high-profile cyberattacks on Target, which led to the CEO stepping down and affected 70 million customers, Target incurred accumulated costs of $252 million by January 2015, of which $90 million was reimbursed by the insurance company, as reported in its 10-K.

[12] This is outlined in Article 6(1), which includes situations of contractual necessity, legal obligation, vital interests, performance of a task carried out in the public interest, or legitimate interests.

[13] The most common GDPR violations are "Insufficient legal basis for data processing" and "Noncompliance with general data processing principles." Available at: https://www.enforcementtracker.com

ifornia Consumer Privacy Act (CCPA), effective January 1, 2020, marks the first comprehensive state-level data privacy regulation. The CCPA imposes fines of $2,500 for unintentional violations and $7,500 for intentional violations, with each affected consumer counting as a separate violation. The CCPA allows California residents to know what types of personal information companies collect and to opt out of data sales. For example, Sephora was fined $1.2 million under the CCPA for allegedly sharing customer data via third-party trackers for advertising and site analytics purposes while falsely claiming not to sell customers' information. Building on the CCPA, the California Privacy Rights Act (CPRA) took effect on January 1, 2023, expanding the scope and penalties. Virginia and Colorado also enacted state privacy laws following California's lead.

In addition, the US Federal Trade Commission (FTC) enforces privacy regulations under Section 5 of the FTC Act, targeting unfair and deceptive data practices. The FTC mandates corrective actions such as implementing privacy programs, conducting biennial privacy assessments, deleting consumer data, and returning unlawful gains. If a firm violates the FTC consent order, the FTC can seek civil penalties per violation. In June 2024, the FTC fined Avast $16.5 million for falsely claiming its software protected users from online tracking while selling consumer browsing data to more than 100 third parties.

2.2 Private enforcement for consumer digital privacy

There has been a surge in various types of consumer privacy lawsuits in the U.S. due to increasing consumer privacy awareness. For example, Google agreed to pay $5 billion in 2023 to settle a consumer privacy class action lawsuit for tracking and collecting personal information in private browsing mode under the Google Chrome browser.[14] Similarly, Meta

[14] Available at:
https://www.reuters.com/legal/google-settles-5-billion-consumer-privacy-lawsuit-2023-12-28/

agreed to pay $90 million for class action settlements in 2022 for tracking Facebook users' online activities through cookies even after they logged out of the platform.[15]

However, litigation concerning consumer privacy has not been limited to tech firms in recent years. Web tracking is broadly costly for various types of firms, and the trend of applying old laws to new technology settings, such as web session replays, has targeted retail firms. For example, according to Bloomberg Law's docket searches, lawsuits for pixel tracking, a type of online tracking, increased by 89 percent from 2022 to 2023.[16] Non-tech firms such as Frontier Airlines, Ray-Ban, and Banana Republic have all been subjected to web-tracking-related class action lawsuits, allegedly violating the Florida Security of Communications Act (FSCA) for tracking website visitors' mouse movements and clicks.[17]

Securities litigation has also emerged regarding firms' approaches to consumer digital privacy, as these practices impact business risk and corporate social responsibility, ultimately influencing investors' valuations. For example, Nielsen Holdings PLC settled a securities class action lawsuit in 2022 for allegedly misrepresenting their readiness for privacy-related regulations, including the GDPR, which would affect their current and future financial performance.[18] Similarly, Direct Digital Holdings, Inc. faced a securities class action lawsuit in 2024 for failing to disclose its inadequate ability to phase out third-party cookies, casting doubt on its positive statements regarding financial performance.[19]

[15] Available at: https://www.reuters.com/technology/metas-facebook-pay-90-million-settle-privacy-lawsuit-over-user-tracking-2022-02-15/

[16] Available at: https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-pixel-privacy-lawsuits-are-up-and-not-just-in-big-tech

[17] See Complaint, Zarnesky v. Frontier Airlines, Inc., No. 6:21-cv-00536 (M.D. Fla. March 24, 2021); Complaint, Goldstein v. Luxottica of Am. Inc., No. 9:21-cv-80546 (S.D. Fla. March 12, 2021); Complaint, Holden v. Banana Republic, LLC, No. 3:21-cv-00268 (M.D. Fla. March 15, 2021).

[18] See Complaint, Gordon v. Nielsen Holdings PLC, No. 18-cv-07143 (S.D.N.Y. August 8, 2018).

[19] See Complaint, Monsky v. Digital Holdings, Inc., No. 24-cv-01940 (S.D. Tex. May 23, 2024).

2.3 Indirect costs of consumer digital privacy

Even if legally permitted, intensive online tracking entails indirect costs that have long-term consequences, such as consumer backlash. Users are often "notified but unaware" of the extent of tracking and data sharing on websites (Larsson et al. 2021). They become aware of this through excessive unsolicited contacts or, worse, when their personal information is transferred among parties to scammers (e.g., Ford 2019), which results in a significant erosion of customers' trust. Such concerns were apparent when Facebook user engagement dropped by 20 percent within a month after its data privacy scandal.[20] Privacy concerns also manifest in reduced purchase likelihood (Pavlou et al. 2007), reluctance to engage with personalized services (Baruh et al. 2017), and a tendency to switch to competitors offering similar services (Martin et al. 2017; Yu et al. 2022). Specifically, Martin et al. (2017) find that 22 percent of respondents switch to competitors when they sense a firm accessing their personal information.

The increased involvement of third parties on websites has introduced security issues. According to Verizon's 2022 Data Breach Investigations Report, 62 percent of all data breaches occur through third-party vendors. This highlights the risks associated with embedding third-party scripts, which can increase susceptibility to cyberattacks (e.g., Urban et al. 2020). Furthermore, Ikram et al. (2019) find that approximately 40 percent of websites implicitly (blindly) trust third parties. Based on IBM's 2024 Cost of a Data Breach Report, the average cost of a data breach is $4.88 million. Third-party tracking, which directly invites third parties to access a firm's website, exposes firms and site visitors to potentially suspicious or malicious actions.

[20] Available at:
https://www.theguardian.com/technology/2019/jun/20/facebook-usage-collapsed-since-scandal-data-show

3 Hypotheses Development

3.1 Main hypotheses

Managers aim to avoid reporting annual earnings decreases because such decreases are often publicly scrutinized (e.g., Burgstahler and Dichev 1997). Firms with consistent earnings growth are typically priced at a premium and may face downward adjustments when this momentum is interrupted (e.g., Myers et al. 2007; Barth et al. 1999; DeAngelo et al. 1996; Lakonishok et al. 1994). Therefore, if managers anticipate not surpassing the previous year's earnings through regular business operations, they may resort to aggressive consumer privacy practices.

Firms face trade-offs when determining their data strategies, including data collection, sharing, and third-party involvement.[21] For example, Karaj et al. (2018) analyze over 1.5 billion page loads and find that firms embed third-party online trackers primarily for advertising and site analytics. Sites offering free editorial content or limited off-site revenue sources (e.g., news sites) tend to embed more trackers to monetize page views. In contrast, sites related to the public sector embed fewer trackers (e.g., Englehardt and Narayanan 2016). Despite the privacy risks associated with public and private enforcement discussed in the previous section, intensified tracking offers a quick and feasible way to extract additional value from existing visitors. There are two primary mechanisms:

Boosting site visits and re-visits: Empirical and anecdotal evidence suggests that personalized and retargeted advertising can significantly increase site traffic in a short period. Firms often target consumers based on their browsing behavior or cart activity, using persistent ads that follow users across the Internet. In an experiment, Sahni et al. (2019) find

[21] Based on my inquiries with tracker operators, the adoption costs of trackers vary widely, ranging from tens to a few thousands of USD per month. Considering that the sample comprises publicly listed firms in the U.S., these adoption costs are relatively modest.

that retargeted users exhibit a 14.6 percent increase in return visits within four weeks. Beyond mere site visits, Manchanda et al. (2006) show that retargeting also enhances purchase probability.

Estimating the direct revenue impact of increased tracking is challenging, as it depends on conversion rates, average order value, and firm size. However, anecdotal evidence from third-party tracker operators suggests that clients can achieve a revenue increase of approximately 20 percent within the first 30 days (see associated costs in the previous section).[22] Additionally, Johnson et al. (2020) estimate that the inability to behaviorally target users who opt out results in an average loss of $8.58 per opt-out consumer in advertising spending. More broadly, prohibiting tracking technologies could reduce advertising effectiveness by approximately 65% (Goldfarb and Tucker 2011) and lead to a 38.5% decline in online publisher revenue (Johnson 2013).

Embedding more third-party trackers on websites expands the reach of a firm's advertising networks. Many advertising intermediaries operating third-party trackers emphasize the breadth of their extensive advertising network and their deals with direct publishers. Third-party trackers also allow firms to merge their customer insights with proprietary datasets from the tracker operators. However, advertising network partners often vary in their aggressiveness toward consumer digital privacy and adherence to privacy regulations, further exposing firms to heightened privacy risks.[23]

Effectiveness of discretionary expenses: Apart from reducing discretionary activities under earnings pressure, firms may shift toward more cost-effective methods. In addition to improving advertising effectiveness, increased tracking intensity for analytical purposes, such as analyzing users' web interactions and mouse clicks, can facilitate product devel-

[22]Examples available at: https://www.criteo.com/success-stories/.

[23]Overall, entering and exiting tracking agreements can vary widely based on the nature of the service. Some trackers offer flexible commitments, such as month-to-month agreements, while others require longer commitments in exchange for lower prices.

opment and differential pricing strategies (e.g., Yousfi and Adelakun 2022; Palmatier et al. 2019). Anecdotal evidence from an online analytics provider shows that web tracking helps identify underutilized software and tools, resulting in cost savings of $805,740 and 2,914 hours saved in internal productivity over three years.[24] These activities affect the overall SG&A and R&D effectiveness. Nonetheless, as discussed in the previous section, the recent trend in privacy litigation shows that new online tracking technologies substantially increase firms' litigation risks.

When traditional EM channels are less feasible, firms may adopt alternative strategies or a mix of techniques to meet earnings benchmarks (e.g., Healy and Wahlen 1999; Cohen et al. 2008; Zang 2012). Intensified third-party online tracking offers a new and hidden way to nudge near-term consumer behavior to reach earnings benchmarks, albeit at the expense of long-term consumers' digital privacy. Defining abnormal tracking as the deviation from the average online tracking levels within the same industry, site category, and year, I state the main hypothesis as follows:

H1: Firms engage in abnormally high third-party online tracking within their domains to beat earnings benchmarks, holding traditional accrual-based and real activity-based earnings management channels constant.

3.2 Costs considerations

3.2.1 The materiality of consumer digital privacy

Abnormally high levels of data collection and sharing expose firms to heightened privacy-related risks. These include regulatory and litigation risks, as well as indirect costs such

[24] Available at:
https://contentsquare.com/blog/total-economic-impact-study-finds-contentsquare-delivered-602-roi-achieving-significant-boost-to-revenue-while-increasing-efficiency-and-customer-happiness/

as consumer backlash. An important consideration is whether these combined risks pose a material threat to the firms. The SASB categorizes firms into 77 industries based on the Sustainable Industry Classification System (SICS) and provides unique sustainability accounting standards for each industry. Among the sustainability-related risks that could materially impact a firm's current or future cash flows, the SASB refers to consumer privacy as the "management of risks related to the use of personally identifiable information (PII) and other customer or user data for secondary purposes." This includes managing issues related to data processing (e.g., collection and sharing), consumers' privacy concerns, and the impact of privacy regulations.

Similar to the Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB), the SASB adopts the materiality interpretation upheld by the U.S. Supreme Court, defined as "a substantial likelihood that the fact would have been viewed by the reasonable investor as having significantly altered the total mix of information made available." [25] Khan et al. (2016) find that firms with good sustainability ratings on SASB industry-specific material issues outperform those without in terms of sustainability investment returns; however, they do not find the same for firms that obtain good ratings on immaterial issues.[26]

For firms in which consumer privacy constitutes a material sustainability risk to their business models, both the capital market and consumers may react strongly to privacy scandals. This is evident in several securities class action lawsuits alleging that firms misrepresented their readiness for privacy regulations, as such information is expected to significantly affect the firm's future financial prospects.[27] The anticipated remediation costs,

[25] TSC Industries v. Northway Inc., 426 U.S. 438, 449 (1976)

[26] To determine materiality, the SASB conducts evidence of materiality tests, including evidence of interest, evidence of financial impacts, and forward impact adjustment (Khan et al. 2016).

[27] See Complaint, Gordon v. Nielsen Holdings Plc, No. 18-cv-07143 (S.D.N.Y. Aug. 8, 2018); Complaint, Monsky v. Digital Holdings, Inc., No. 24-cv-01940 (S.D. Tex. May 23, 2024).

long-term reputational damage, and heightened scrutiny drive investors' and consumers' reactions to privacy scandals. On the other hand, if these firms effectively manage consumer privacy, they will foster consumer loyalty and attract privacy-conscious consumers from competitors (e.g., Martin et al. 2017). Based on this argument, I propose the following hypothesis:

H2a: Firms' use of abnormal tracking to beat earnings benchmarks is mitigated when consumer privacy constitutes a material sustainability risk.

3.2.2 Data governance

Data governance broadly refers to exercising authority and control over data management (Abraham et al. 2019). This concept encompasses data strategies, policies, and monitoring practices designed to maximize the value of data while managing data-related risks (Abraham et al. 2019; Borgman et al. 2016). The costs associated with abnormal tracking are greater when a firm publicly designates a board committee to oversee its data practices because, if the firm does otherwise, its public statement could be considered misleading and potentially lead to litigation. Additionally, the board may pose more informed questions regarding the firm's privacy practices and directly restrict the suboptimal use of trackers.

Previous studies show that a board's monitoring role mitigates earnings management (e.g., Klein 2002) and facilitates the implementation of business ethics codes of conduct (e.g., García-Sánchez et al. 2015). Given that more business decisions now involve cyber components as well as environmental, social, and governance (ESG) considerations, the board's role in overseeing enterprise risks, as endorsed by the SEC and the Committee of Sponsoring Organizations (COSO), extends to managing risks related to the cyber and ESG domains. For example, Uber's 2020 proxy statement noted that they "formally added oversight of data privacy to the charter of the Board's Audit Committee." Similarly, Klein et al. (2022) demonstrate that, following the EU GDPR, U.S. boards tend to increase their focus on cyber risks and add more information technology (IT) experts to the board. Consequently, the board committee responsible for privacy oversight is expected to develop a better understanding of firms' data privacy policies. Based on this argument, I propose the following hypothesis:

H2b: Firms' use of abnormal tracking to beat earnings benchmarks is mitigated when board committees are tasked with privacy oversight.

4 Research Design

4.1 Sample construction

Online tracking refers to the practice of collecting Internet users' information as they navigate online (Karaj et al. 2018; Mayer and Mitchell 2012). To assess third-party tracking intensity within a firm's domain, I obtained data from Whotracks.me, which monitors thousands of websites and provides insights into third-party tracker usage.[28] I manually matched all sites in the July 2022 file to their respective owners and the parent companies' NYSE or NASDAQ tickers using Capital IQ.[29] I began with the July 2022 file, as it was the most recent data available at the project's inception.[30] Whotracks.me defines a tracker as a

[28]Karaj et al. (2018) provide detailed explanations of how Whotracks.me identifies online trackers, and Lukic et al. (2023) use Whotracks.me data to examine the impact of GDPR on online tracking.

[29]I search for the site, with or without the top-level domain (TLD), to obtain tickers of the site owners in Capital IQ. If the search results are ambiguous, I use the "ipwhois" Python package to identify the domain owner.

[30]To make the panel data collection manageable, for each site with an identified ticker in the July 2022 folder, I retroactively search for tracker usage within the July 2021, 2020, 2019, and 2018 files to construct an annual panel dataset. Thus, the tracker usage in July of each year represents the tracker usage for that fiscal year.

third-party domain that appears on multiple websites and utilizes cookies or fingerprinting methods to transmit user identifiers. I exclude sites that are not owned by publicly listed companies or lack the required data in Compustat.[31]

Next, I use the SICS lookup tool on the SASB website to determine a firm's SICS industry. The SASB categorizes firms into industries according to their business models and sustainability impacts. According to the SASB, there are six industries where customer privacy constitutes a material sustainability risk: E-commerce, Consumer Finance, Internet Media & Services, Software & IT Services, Advertising & Marketing, and Telecommunication Services. After satisfying the requirements for calculating the main variable $Ab\_trackers$ in the next section, as well as the firm-level controls, the final panel dataset spans July 2018 to July 2022 and comprises 2,401 site-year observations, all of which fall within the post-GDPR period.

To identify the board committee's responsibility for consumer privacy oversight, I analyze DEF 14A proxy statements filed in the same year as the tracker data.[32] I read through the paragraphs that include the keyword "privacy" to determine whether a committee is explicitly tasked with overseeing consumer privacy. Instead of simply counting the occurrences of the word "privacy," this approach excludes boilerplate language, ensuring that statements which do not assign accountability for privacy violations are not included (e.g.,"our company has made commitments on issues concerning the public, such as consumer privacy"). Committees responsible for privacy oversight are often audit committees, risk committees, and privacy or technology committees.[33]

[31] The status of each site's parent company was determined in December 2022.

[32] I search the Electronic Data Gathering, Analysis, and Retrieval (EDGAR) index files for entries with form type equal to DEF 14A.

[33] The information typically appears in the chart of the proxy statement that outlines the responsibilities of each board committee.

4.2 Measuring abnormal tracking and suspected earnings management

I measure each site's "abnormal" third-party tracking intensity by the deviation from the mean tracking intensity within the same industry, site category, and year. The industry-category-year grouping is necessary because the normal level of online tracking varies significantly across industries (e.g., manufacturing versus e-commerce), site categories (e.g., news sites versus business sites), and years (e.g., changes in the regulatory environment).

To ensure a sufficient sample size and a meaningful average for each group, at least 15 observations for each group were required.[34] Abnormal tracking ($Ab\_trackers$) is calculated as follows.

$$Average\_trackers_{i,t} = Mean\, trackers(SASB\_industry_i, Site\_category_i, Year_t) \quad (1)$$

$$Ab\_trackers_{i,t} = Trackers_{i,t} - Average\_Trackers_{i,t} \quad (2)$$

I identify firms suspected of managing earnings to avoid earnings decreases based on Burgstahler and Dichev (1997)'s finding that firms exhibit earnings changes just above zero. Specifically, $Suspect$ equals one if changes in earnings, deflated by the beginning-of-the-year total assets, fall within the range [0, 0.0025), the interval used by Burgstahler and Dichev (1997). I also deflate changes in earnings by net sales to generate an alternative $Suspect$ variable for the robustness tests.

4.3 Model specifications: Baseline regression

To test the main hypotheses on consumer digital privacy and earnings benchmarks, I estimate the following baseline OLS regression model. I employ OLS regression instead

[34] Roychowdhury (2006) requires at least 15 observations for each industry-year group when estimating "abnormal" cash flows, cost of goods sold, inventory growth, production costs, and discretionary expenses.

of a count model because tracking intensity from Whotracks.me is a continuous variable representing the average number of third-party trackers per page load on the website. Additionally, I include site fixed effects to examine within-site variations, thereby controlling for unobservable site-level factors that are constant over time but may influence tracking intensity.

While site fixed effects in equation (3) allow for interpreting the coefficient on $Suspect$ compared to the site's average tracking intensity, I directly examine changes in trackers for parsimony in equation (4) and control for other higher-order fixed effects.

$$\begin{aligned} Ab\_trackers_{i,t} = \beta_1 Suspect_{i,t} + \sum EM\_proxies_{i,t} + \sum Controls_{i,t} \\ + Site\_FE + Year\_FE + \epsilon_{i,t} \end{aligned} \tag{3}$$

$$\Delta Trackers_{i,t} = \beta_1 Suspect_{i,t} + \sum EM\_proxies_{i,t} + \sum Controls_{i,t} + FEs + \epsilon_{i,t} \tag{4}$$

where $Suspect$ equals 1 for firms that just exceed the previous year's earnings and 0 otherwise. $EM\_proxies$ include conventional earnings management proxies, constructed such that higher values indicate greater earnings management. To account for firm characteristics that potentially affect both online tracking and the extent of changes in earnings, I control for the natural logarithm of total assets ($Size$), debt divided by beginning total assets (Lev), sales divided by beginning total assets ($Turnover$), capital expenditures divided by beginning total assets ($CAPEX$), and whether the site has a foreign top-level domain ($Site\_foreign$).[35] A positive β_1 in equation (3) would indicate a positive association between meeting or barely beating a target and unusually high third-party tracking,

[35] It is difficult to list all possible top-level domains as they could vary by country. Thus, I code a site as foreign if its top-level domain is other than .us, .com, or .org.

supporting the hypothesis that firms engage in unusually high third-party tracking to avoid earnings decreases. Similarly, a positive β_1 in equation (4) suggests a positive association between suspect firms and an increased use of third-party trackers.

4.4 Model specifications: Cost considerations

This section examines two cross-sectional variations in the costs of overlooking consumer digital privacy: (1) the materiality of consumer privacy as a sustainability risk and (2) board committee privacy oversight. To explore the mitigating effect of materiality considerations, I estimate the OLS regression below.[36]

$$\begin{aligned} Ab\_trackers_{i,t} = {} & \beta_0 Suspect_{i,t} + \beta_1 Suspect_{i,t} \times SASB\_material_{i,t} \\ & + \sum EM\_proxies_{i,t} + \sum Controls_{i,t} + FEs + \epsilon_{i,t} \end{aligned} \tag{5}$$

where $SASB\_material$ equals one if the SASB deems customer privacy a material sustainability risk for the sector in which the firm operates, and zero otherwise. A negative β_1 supports hypothesis H2a that consumer privacy, when constituted as a material sustainability risk to the firm's cash flow, mitigates the tendency to engage in abnormal tracking to avoid missing earnings benchmarks.

To test the mitigating effect of the board committee's privacy oversight, I estimate the following OLS regression:

$$\begin{aligned} Ab\_trackers_{i,t} = {} & \beta_0 Suspect_{i,t} + \beta_1 Suspect_{i,t} \times Board\_privacy_{i,t} \\ & + \beta_2 Board\_privacy_{i,t} + \sum EM\_proxies_{i,t} + \sum Controls_{i,t} + FEs + \epsilon_{i,t} \end{aligned} \tag{6}$$

where $Board\_privacy$ equals one if a board committee is responsible for overseeing con-

[36] Since $SASB\_material$ does not vary within site/firm, it is absorbed by the site/firm fixed effects and, therefore, not separately identified.

sumer privacy, as indicated in the DEF14A proxy statement, and zero otherwise. A negative β_1 supports the hypothesis (H2b) that board committee privacy oversight mitigates firms' tendency to overlook consumer privacy to sustain earnings growth.

5 Empirical Results

5.1 Descriptive statistics

Panel A of Table 1 presents the distribution of site categories within the sample, following the site categorization in Karaj et al. (2018). Of these sites, 42.69 percent belong to the business-related category, 14.41 percent are classified as e-commerce, and 17.87 percent are related to entertainment. News and portal sites have the highest average number of third-party trackers at 18.7, followed by entertainment sites at 8.96, and recreation sites at 8.4. Reference sites have the lowest average number of third-party trackers at 2.91. Trackers related to owned products (e.g., retailers driving traffic to their own online sales) are often prevalent on e-commerce and business sites. In contrast, trackers related to others' products are most commonly used on news and portal sites, which rely heavily on advertising revenue by selling ad space to various advertisers.

Panel B of Table 1 shows the distribution of the SICS industries by the SASB at the firm level. Internet Media & Services (33.74 percent), Software & IT Services (29.45 percent), and E-commerce (14.41 percent) emerge as the top three SICS industries. The SICS classification allows for the determination of whether customer privacy is material to the firm. Among the eight SICS industries in the sample, consumer privacy is considered material in four (E-commerce, Internet Media & Services, Software & IT Services, and Telecommunication Services). The media and entertainment industry has the most third-party trackers, averaging 16.98, followed by multi-line and specialty retailers and distributors at 13.02.

Panel C of Table 1 presents the distribution of the sample years. In 2018, the first year of the sample, the average number of trackers is the lowest. Panel D of Table 1 shows the distribution of board committees responsible for overseeing consumer digital privacy. Among the 61 percent of the sample with a board committee designated for privacy oversight, 76.77 percent are overseen by the audit committee, 13.94 percent by the risk and regulatory committee, 5.95 percent by the privacy committee, 1.06 percent by the technology or security committee, and 2.28 percent by others.

(Insert Table 1 about here)

Panel A of Table 2 provides summary statistics for site-level variables. I winsorize all continuous variables at the top and bottom one percent. The final sample consists of 2,401 site-year observations across 834 unique firm-years. The average number of trackers is 7.54. By construction, the mean number of abnormal trackers ($Ab\_trackers$) is 0. The median site has a $Site\_foreign$ value of 0, indicating a non-foreign TLD.

Panel B of Table 2 provides summary statistics for firm-level variables. Approximately half of the observations come from firms in SICS industries where consumer privacy constitutes a material sustainability risk ($SASB\_privacy$). The median firm size ($Size$), calculated as the logarithm of total assets, is 9.87, indicating that the median firm has total assets of approximately \$19 billion. Moreover, the median firm exhibits a leverage (Lev) of around 66 percent, a sales turnover ratio ($Turnover$) of approximately 66 percent, and capital expenditure ($CAPEX$) of around 3 percent of beginning total assets. Additionally, 61 percent of the firms in the sample have a board committee responsible for overseeing consumer privacy ($Board\_privacy$).

Panel C of Table 2 presents the summary statistics for the conventional EM proxies. The median firm exhibits levels of abnormal changes in working capital accruals (Ab_wc_chg)

and abnormal operating cash flows (Ab_ocf) similar to the sample mean. However, the median firm shows higher levels of discretionary accruals (Ab_tacc) and overproduction (Ab_prod), but lower levels of discretionary expense (Ab_disexp) compared to the sample mean.

(Insert Table 2 about here)

Table 3 presents the Pearson correlations between abnormal tracking ($Ab\_trackers$) and the other variables. The correlations reveal that $Ab\_trackers$ is negatively and significantly correlated with abnormal accruals (Ab_tacc), abnormal operating cash flows (Ab_ocf), size ($Size$), capital expenditures ($CAPEX$), foreign domain ($Site\_foreign$), and board committee privacy oversight ($Board\_privacy$). Conversely, $Ab\_trackers$ is positively and significantly correlated with abnormal discretionary expense (Ab_disexp), leverage (Lev), and turnover ($Turnover$). These correlations suggest that, in terms of firm characteristics, smaller firms, firms with lower capital expenditures, leveraged firms, high-turnover firms, and firms without board committee privacy oversight exhibit higher levels of abnormal tracking. Moreover, the correlation matrix provides preliminary evidence that abnormal online tracking may be used as a substitute when conventional EM channels are limited, except for abnormal discretionary expenses EM, which can be complemented by consumer online tracking.

(Insert Table 3 about here)

5.2 The validity and characteristics of the abnormal tracking measure

Before testing the main predictions, I test the validity and characteristics of the main abnormal tracking measure ($Ab\_trackers$). First, I examine whether heightened consumer privacy regulations are associated with less abnormal tracking ($Ab\_trackers$). To achieve this, I implement a difference-in-differences design using the California Consumer Privacy

Act (CCPA) as an exogenous shock. The CCPA, the first comprehensive consumer privacy state law in the US, came into effect in January 2020. $Treat$ equals 1 for U.S. firms ($Site\_foreign$ equals 0) and 0 for Canadian sites (with TLD ending in .ca). $Post$ equals 1 for the years 2020 and 2021, and 0 for the years 2018 and 2019.[37] I then estimate the following OLS regression:

$$Ab\_trackers_{i,t} = \beta_1 Treat_{i,t} + \beta_2 Post_{i,t} + \beta_3 Treat_{i,t} \times Post_{i,t} + \sum Controls_{i,t} + FEs + \epsilon_{i,t} \tag{7}$$

Columns (1) and (2) of Table 4 present the difference-in-differences results for $Ab\_trackers$. The coefficient on $Treat \times Post$ is significantly negative, indicating that after the CCPA came into effect, $Ab\_trackers$ of U.S. sites dropped significantly compared to Canadian sites, both with and without controls. The results support the validity of the main variable, $Ab\_trackers$.[38]

Second, I examine the characteristics of abnormal tracking ($Ab\_trackers$), focusing on its relation with conventional EM methods by estimating the following OLS regression:

$$Ab\_trackers_{i,t} = EM\_proxy_{i,t} + \sum Controls_{i,t} + FEs + \epsilon_{i,t} \tag{8}$$

Following Ham et al. (2017), I analyze five commonly used EM proxies: the absolute value of discretionary accruals (Ab_tacc) from the modified Jones (1991) model, modified by Dechow et al. (1995) and Kothari et al. (2005); the abnormal change in working capital accruals (Ab_wc_chg) proposed by Dechow and Dichev (2002) and modified by McNichols (2002); and three real earnings management proxies from Roychowdhury (2006), including abnormal discretionary expenses (Ab_disexp), abnormal cash flows from operations (Ab_ocf), and abnormal production costs (Ab_prod).

[37] I do not include sites with European TLDs because those sites have already been subject to the influential GDPR since 2018, and my sample is post-GDPR.

[38] The variables $Treat$ and $Post$ are absorbed by the site fixed effects and are therefore not identified.

Columns (3)-(7) of Table 4 present the relation between $Ab\_trackers$ and the five conventional EM proxies. Abnormal tracking ($Ab\_trackers$) is negatively associated with total accruals (Ab_tacc), abnormal working capital accruals (Ab_wc_chg), and overproduction (Ab_prod). The findings are reasonable in the digital-based new economy, where the relevance of production may diminish for firms operating within service-oriented models. Similarly, firms with straightforward revenue recognition processes may have minimal accruals.

Interestingly, abnormal tracking is positively and significantly associated with discretionary expenses (Ab_disexp), implying that intensified tracking complements discretionary expenses. Specifically, when firms exhibit abnormal cuts in discretionary spending, they tend to become more aggressive in their consumer digital privacy practices to enhance the effectiveness of their existing advertising, R&D, and SG&A expenditures.

(Insert Table 4 about here)

5.3 Consumer digital privacy and earnings benchmarks

Table 5 presents the relation between suspect firms and abnormal third-party tracking (H1) by estimating equations (3) and (4). Columns (1) and (2) of Table 5 present the results with abnormal trackers ($Ab\_trackers$) as the dependent variable and include site-level fixed effects to examine within-site variations. The significantly positive coefficient on $Suspect$ indicates that suspect firms exhibit significantly higher abnormal tracking intensity within their domains, even after controlling for existing accrual-based and real activity-based EM channels. This finding implies that abnormal online tracking is more than a proxy for conventional EM practices.

Column (3) presents the results using changes in trackers ($\Delta Trackers$) as the dependent variable. The significantly positive coefficient on $Suspect$ indicates that suspect firms increase the number of trackers relative to non-suspect firms. Regarding economic significance, column (2) of Table 5 shows that suspect firm years are associated with 1.48 more abnormal trackers than non-suspect firm years. In column (3), which directly examines the change in trackers, suspect firm years are associated with a 1.57 increase in trackers. The change in trackers represents approximately 20 percent of the mean tracker usage of 7.54, as reported in the summary statistics.

(Insert Table 5 about here)

5.4 Cost considerations: Materiality

Table 6 presents the results on whether firms' tendency to engage in abnormal tracking to meet earnings benchmarks is mitigated when consumer privacy constitutes a material sustainability risk. Materiality considerations encompass both the direct and indirect costs associated with abnormal tracking. The coefficients on the interaction term between $Suspect$ and $SASB\_material$ in columns (1) and (2) are significantly negative.[39] The results are consistent with the hypothesis that firms in industries where consumer privacy poses a material risk to current and future cash flows are significantly less likely to compromise privacy in order to avoid missing earnings benchmarks. This finding remains statistically significant in column (3), where $\Delta Trackers$ is the dependent variable. The coefficient on $Suspect \times SASB\_material$ in column (2) demonstrates the economic significance of the findings, indicating that suspect firms with customer privacy as a material sustainability risk are associated with approximately 78 percent lower abnormal tracking than other suspect firms.

(Insert Table 6 about here)

[39]The indicator for materiality does not vary over time; thus, $SASB\_material$ is absorbed by the site/firm fixed effects and is therefore not reported.

5.5 Cost considerations: Board committee privacy oversight

Table 7 presents the results of estimating the mitigating impact of board committee oversight on firms' tendency to overlook consumer privacy to avoid missing benchmarks. The coefficients on the interaction term $Suspect \times Board\_privacy$ in columns (1) and (2) are both significantly negative. The results are consistent with the hypothesis that firms with a board committee responsible for consumer privacy are significantly less likely to compromise digital privacy under earnings pressure. This result is also statistically significant in column (3) when $\Delta Trackers$ is examined as the dependent variable.

The findings in Table 7 are economically significant, as indicated by the coefficient on $Suspect \times Board\_privacy$ in column (2), which suggests that suspect firms with board committee privacy oversight are associated with approximately 76 percent lower abnormal tracking than suspect firms without committee oversight. Given that the sample period is post-GDPR, the results build on the findings of Klein et al. (2022) by demonstrating that U.S. firms not only alter their board compositions in response to GDPR, but also enhance their data governance practices through the oversight of board committees. Moreover, these findings challenge the notion that intensive tracking is the best practice, as firms' own data governance mechanisms reduce such behavior.

(Insert Table 7 about here)

5.6 Test of mechanisms

I examine whether abnormal tracking enables firms to reach earnings benchmarks via two mechanisms: (1) boosting site popularity ($Popular$) via an expanded advertising network with personalized content, and (2) increasing the effectiveness of discretionary expenses ($Disc\_effective$). Columns (1) and (2) of Table 8 present the results of testing whether increased site popularity serves as a mechanism through which suspect firms meet benchmarks through abnormal tracking. The coefficients on the interaction term $Suspect \times Popular$ in both columns are significantly positive. These findings suggest that the associations between $Suspect$ and $Ab\_trackers$, as well as between $Suspect$ and $\Delta Trackers$, are stronger when the suspect firm achieves high site popularity.

Columns (3) and (4) of Table 8 present the results of examining whether increased discretionary expense effectiveness serves as a mechanism by which suspect firms meet earnings benchmarks through abnormal tracking. The coefficients on the interaction term $Suspect \times Disc\_effective$ in both columns are positive and significant, supporting the notion that the relation between earnings benchmarks and abnormal tracking is more pronounced when a suspect firm exhibits highly effective discretionary spending. Taken together, the mechanisms in Table 8 illustrate the benefits of abnormally aggressive consumer digital privacy practices, which enable firms to extract additional value from existing customers at the expense of their privacy.

(Insert Table 8 about here)

5.7 Additional tests: Analysts forecasts as an alternative benchmark

This section re-examines the main hypothesis by using consensus analyst annual EPS forecasts as an alternative earnings benchmark. Following Caskey and Ozel (2017), I define $Suspect\_ibes$ as firms that exceed the average analyst forecast by two cents or less. I include annual forecasts issued within 90 days prior to the earnings announcement. Columns (1) and (2) in Table 9 indicate that firms narrowly beating analyst forecasts ($Suspect\_ibes$) engage in significantly higher levels of third-party tracking within their domains. This finding holds in column (3), which further controls for conventional EM channels.

Compared to the main finding in Table 5, the economic magnitude is about half when analyst forecasts are used as benchmarks rather than the prior year's earnings. One possible reason is that prior-year earnings serve as a static and thus more easily beatable benchmark, reflecting historical data that remains unchanged after reporting. By contrast, analyst forecasts provide a more dynamic benchmark, updating based on new information or changing market conditions. Another possibility is that trackers are stickier than analyst forecasts.[40]

(Insert Table 9 about here)

5.8 Robustness tests

Table 10 presents the results of replicating the main findings using alternative methods to identify suspect firms and abnormal trackers. Columns (1) to (3) replicate the findings using net sales as an alternative deflator for earnings changes to identify suspect firms. This approach generates an alternative group of suspect firms ($Suspect\_sale$) that fall within the interval [0, 0.0025). In column (1), suspect firm-years ($Suspect\_sale$) exhibit significantly higher levels of abnormal tracking ($Ab\_trackers$) compared to non-suspect firm-years. The coefficient on the interaction term $SASB\_material \times Suspect\_sale$ in column (2) replicates the finding that the relation between suspect firms and $Ab\_trackers$ is significantly less pronounced when consumer privacy constitutes a material sustainability risk ($SASB\_material$). The coefficient on the interaction term $Board\_privacy \times Suspect\_sale$ in column (3) suggests that suspect firms with a board committee responsible for consumer privacy oversight ($Board\_privacy$) are significantly less likely to overlook digital privacy to meet earnings benchmarks.

(Insert Table 10 about here)

[40] The results are insignificant in untabulated analyses that use the consensus quarterly EPS forecast as the earnings benchmark. This may stem from the use of annual data for trackers, collected each July. For example, analysts have forecasted a calendar year company's Q3 and Q4 earnings after the July collection of tracker data. To the extent that analyst forecasts reflect their estimates of tracking activity, there should be no relation between Q3 and Q4 earnings surprises and the July tracker usage.

6 Conclusion

This study examines whether earnings benchmarks influence firms' aggressiveness toward consumer digital privacy, holding the conventional accrual-based and real activities-based earnings management channels constant. I find that firms that just beat annual earnings benchmarks exhibit abnormally high levels of third-party tracking within their domains compared to other firms, even after controlling for traditional EM methods. Additionally, online tracking intensifies when traditional earnings management channels are less feasible.

The study validates two mechanisms through which firms at risk of missing benchmarks benefit from abnormal tracking: (1) increasing site visits through expanded advertising networks and personalized ads, and (2) enhancing the effectiveness of discretionary expenses. The main finding is less pronounced for firms in industries where consumer privacy is a material sustainability risk (as per the SASB classification) and for those with a board committee overseeing consumer privacy (based on their proxy statement disclosures).

Overall, this study broadens our understanding of how firms react to earnings benchmarks in an increasingly important yet often hidden digital space, as well as how EM strategies evolve over time, impacting a wide range of stakeholders through the Internet.

Appendix A: Variable Definitions

Variable	Description
Trackers	The average number of third-party trackers per page load within the website. The third-party tracking data is from Whotracks.me.
Ab_trackers	The abnormal level of third-party tracking, calculated as the deviation from the mean within the SICS industry, site category, and year.
Suspect	Equal to one if changes in earnings deflated by the beginning-of-the-year total assets fall within the range [0,0.0025), the interval used by Burgstahler and Dichev (1997), and zero otherwise.
SASB_material	Equal to one if customer privacy is considered material for the sector in which the firm operates, and zero otherwise (SASB).
Board_privacy	Equal to one if a board committee is explicitly responsible for overseeing consumer privacy (DEF14A), and zero otherwise.
Size	The natural logarithm of the total assets at the beginning of the year.
Lev	Total liabilities divided by the beginning of the year total assets.
Turnover	Net sales divided by the beginning of the year total assets.
CAPEX	Capital expenditures divided by the beginning of the year total assets.
Site_foreign	Equal to one if the top-level domain of the site is not ".us, .com, or .org," and zero otherwise.
Popular	The site's popularity categorized into high, medium, and low each year.
Disc_effective	Sales per SG&A categorized into high, medium, and low each year.
Ab_tacc	The absolute value of discretionary accruals from the modified Jones (1991) model, refined by Dechow et al. (1995) and Kothari et al. (2005).
Ab_wc_chg	Abnormal change in working capital accruals proposed by Dechow and Dichev (2002), as modified by McNichols (2002).
Ab_prod	Abnormal production costs proposed by Roychowdhury (2006).
Ab_disexp	Abnormal discretionary expenses from Roychowdhury (2006) multiplied by negative one to ensure higher values indicate higher EM.
Ab_ocf	Abnormal cash flows from operations from Roychowdhury (2006) multiplied by negative one to ensure higher values indicate higher EM.
Suspect_ibes	Equal to one if firms exceed the mean analyst forecast by two cents or less within 90 days before the earnings announcement; zero otherwise.

Appendix B: Examples of third-party trackers

The following code snippets provide examples of Google Analytics and Google AdSense.

```
***Google Analytics***
<script async src="https://www.googletagmanager.com/gtag/js?
id=G-R7G2******"></script>
<script>
  window.dataLayer = window.dataLayer || [];
  function gtag(){dataLayer.push(arguments);}
  gtag('js', new Date());
  gtag('config', 'G-R7G2******');
</script>
***Google AdSense***
<script async src="https://pagead2.googlesyndication.com/pagead/js
/adsbygoogle.js?
client=ca-pub-4556732768******"
    crossorigin="anonymous"></script>
<!-- ad2 -->
<ins class="adsbygoogle"
    style="display:block"
    data-ad-client="ca-pub-4556732768******"
    data-ad-slot="4570******"
    data-ad-format="auto"
    data-full-width-responsive="true"></ins>
<script>
    (adsbygoogle = window.adsbygoogle || []).push({}); </script>
```

Tables

Table 1: Sample Composition

Panel A. Site Category		Freq.	Percent	Trackers
Business		1,025	42.69	7.2
E-Commerce		346	14.41	6.91
Entertainment		429	17.87	8.96
News and Portals		122	5.08	18.70
Recreation		166	6.91	8.40
Reference		313	13.04	2.91
Panel B. SICS industry	**Materiality**	**Freq.**	**Percent**	**Trackers**
E-Commerce	Y	346	14.41	6.91
Hardware	N	73	3.04	6.05
Internet Media & Services	N	810	33.74	5.49
Media & Entertainment	Y	238	9.91	16.98
Multiline and Specialty Retailers & Distributors	N	118	4.91	13.02
Professional & Commercial Services	N	64	2.67	8.00
Software & IT Services	Y	707	29.45	6.32
Telecommunication Services	Y	45	1.87	7.96
Panel C. Year distribution		**Freq.**	**Percent**	**Trackers**
2018		159	6.62	6.34
2019		489	20.37	8.33
2020		564	23.49	7.66
2021		587	24.45	6.84
2022		602	25.07	7.93
Panel D. Board committees for privacy oversight			**Freq.**	**Percent**
Audit Committee			942	76.77
Risk / Regulatory Committee			171	13.94
Privacy Committee			73	5.95
Technology / Security Committee			13	1.06
Others			28	2.28

Table 2: Summary Statistics

Panel A. Site-level variables	N	mean	sd	p10	p25	p50	p75	p90
Trackers	2401	7.54	5.61	2.05	3.16	5.95	10.13	15.43
Ab_trackers	2401	0.00	4.14	-4.36	-2.75	-0.77	2.04	5.63
Site_foreign	2401	0.32	0.47	0.00	0.00	0.00	1.00	1.00
Panel B. Firm-level variables								
SASB_material	2401	0.56	0.50	0.00	0.00	1.00	1.00	1.00
Suspect	2401	0.01	0.11	0.00	0.00	0.00	0.00	0.00
Size	2401	9.90	2.12	7.05	8.24	9.87	12.13	12.67
Lev	2401	0.70	0.37	0.31	0.41	0.66	0.88	1.10
Turnover	2401	0.81	0.57	0.34	0.47	0.66	0.86	1.49
CAPEX	2401	0.04	0.04	0.01	0.01	0.03	0.07	0.10
Board_privacy	2021	0.61	0.49	0.00	0.00	1.00	1.00	1.00
Panel C. Conventional EM proxies								
Ab_tacc	2310	0.01	0.12	-0.11	-0.04	0.02	0.07	0.14
Ab_wc_chg	2260	-0.01	0.05	-0.06	-0.03	-0.01	0.01	0.04
Ab_prod	2214	-0.10	0.15	-0.29	-0.18	-0.09	-0.03	0.06
Ab_ocf	2394	0.17	0.16	-0.02	0.06	0.17	0.28	0.37
Ab_disexp	2351	-0.06	0.35	-0.39	-0.33	-0.12	0.10	0.35

Table 3: Correlation Matrix

Correlations significant at the 10 percent level are in bold.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)
Ab_trackers (1)	1.00												
Ab_tacc (2)	**-0.04**	1.00											
Ab_wc_chg (3)	0.01	**0.44**	1.00										
Ab_prod (4)	-0.02	**0.15**	**0.10**	1.00									
Ab_ocf(5)	**-0.07**	0.00	**-0.17**	**-0.37**	1.00								
Ab_disexp (6)	**0.14**	**-0.49**	**-0.16**	**-0.43**	**-0.23**	1.00							
Size (7)	**-0.26**	**0.24**	0.03	**0.16**	**0.24**	**-0.51**	1.00						
Lev (8)	**0.08**	**-0.35**	**-0.20**	**-0.16**	**-0.10**	**0.38**	**-0.33**	1.00					
Turnover (9)	**0.05**	**-0.23**	**-0.14**	**-0.07**	**0.13**	**0.31**	**-0.16**	**0.38**	1.00				
CAPEX (10)	**-0.10**	0.00	**-0.12**	**-0.10**	**0.34**	-0.02	**0.46**	**-0.04**	**0.35**	1.00			
Site_foreign (11)	**-0.19**	-0.03	-0.02	-0.02	**0.13**	**-0.04**	**0.30**	**-0.20**	-0.02	**0.26**	1.00		
Board_privacy (12)	**-0.16**	0.00	**-0.11**	**-0.16**	**0.36**	**-0.13**	**0.47**	**-0.18**	-0.03	**0.35**	**0.35**	1.00	
SASB_material (13)	0.00	**-0.12**	**-0.13**	**0.08**	**-0.12**	**0.08**	**-0.10**	**0.27**	**-0.07**	**-0.11**	**-0.21**	**-0.11**	1.00

Table 4: The validity and characteristics of abnormal tracker ($Ab\_trackers$)

Table 4 reports the results of validity and characteristic tests for abnormal trackers ($Ab\_trackers$).Columns (1) and (2) present the results of the difference-in-differences test, using the CCPA as an exogenous shock. Treat equals one for U.S. firms and zero for Canadian sites. Post equals one for the years 2020 and 2021, and zero for the years 2018 and 2019. Columns (3) through (7) examine the relation between $Ab\_trackers$ and other conventional EM proxies. t-statistics are reported in parenthesis. Appendix A provides variable definitions. Two-tailed significance levels are denoted by: *** 1 percent, ** 5 percent, and * 10 percent.

	Regulatory shock		Relation with traditional EM channels				
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
VARIABLES	Ab_trackers	Ab_trackers	Ab_trackers	Ab_trackers	Ab_trackers	Ab_trackers	Ab_trackers
Treat × Post	-1.663**	-1.528**					
	(-2.23)	(-2.05)					
Ab_tacc			-0.022				
			(-0.04)				
Ab_wc_chg				-1.773			
				(-1.59)			
Ab_prod					-1.593**		
					(-2.08)		
Ab_ocf						0.330	
						(0.60)	
Ab_disexp							1.083***
							(3.22)
Constant	1.412***	5.184	2.724	2.127	-0.060	2.995	1.075
	(3.00)	(1.34)	(1.00)	(0.77)	(-0.02)	(1.20)	(0.43)
Controls	No	Yes	Yes	Yes	Yes	Yes	Yes
Observations	1,247	1,247	2,286	2,233	2,183	2,384	2,340
R-squared	0.828	0.829	0.805	0.805	0.812	0.808	0.812
Fixed effects	Site&Year	Site&Year	Site&Year	Site&Year	Site&Year	Site&Year	Site&Year

Table 5: The relation between consumer digital privacy and earnings benchmarks

Table 5 reports the results of examining the relation between consumer digital privacy and earnings benchmarks. Columns (1) and (2) present the results using $Ab\_trackers$ as the dependent variable, while Column (3) presents the result using $\Delta Trackers$ as the dependent variable. t-statistics are reported in parenthesis. Appendix A provides variable definitions. Ind. denotes industry and Cat. denotes website category. Two-tailed significance levels are denoted by: *** 1 percent, ** 5 percent, and * 10 percent.

VARIABLES	(1) Ab_trackers	(2) Ab_trackers	(3) $\Delta Trackers$
Suspect	1.420***	1.483***	1.570***
	(3.26)	(3.54)	(2.70)
Size	-0.298	0.176	-0.544
	(-1.29)	(0.68)	(-1.13)
Lev	0.117	0.719**	-0.466
	(0.45)	(2.20)	(-0.85)
Turnover	-0.609*	-0.770**	0.222
	(-1.92)	(-1.99)	(0.35)
CAPEX	7.707**	6.100*	-4.256
	(2.47)	(1.92)	(-0.76)
Site_foreign			0.011
			(0.05)
Ab_wc_chg		-0.693	-2.328
		(-0.64)	(-1.41)
Ab_disexp		0.809**	-0.604
		(2.24)	(-1.02)
Ab_prod		-1.995**	-3.674***
		(-2.55)	(-2.74)
Constant	3.008	-2.255	5.226
	(1.22)	(-0.81)	(1.00)
Observations	2,393	2,099	1,659
R-squared	0.810	0.819	0.190
Fixed effects	Site&Year	Site&Year	Firm&Cat.&Year

Table 6: Cost considerations: SASB materiality

Table 6 presents the mitigating effects of materiality on abnormal tracking in suspect firm-years. Columns (1) and (2) present the results with $Ab\_trackers$ as the dependent variable, while Column (3) presents the results with $\Delta Trackers$ as the dependent variable. t-statistics are reported in parenthesis. Appendix A provides variable definitions. Ind. denotes industry and Cat. denotes website category. Two-tailed significance levels are denoted by: *** 1 percent, ** 5 percent, and * 10 percent.

VARIABLES	(1) Ab_trackers	(2) Ab_trackers	(3) $\Delta Trackers$
Suspect × SASB_material	-2.497*** (-2.62)	-2.525*** (-2.80)	-3.657*** (-2.89)
Suspect	3.218*** (3.99)	3.238*** (4.30)	4.125*** (3.90)
SASB_material	-	-	-
Size		0.231 (0.89)	-0.412 (-0.85)
Lev		0.758** (2.32)	-0.364 (-0.67)
Turnover		-0.792** (-2.05)	0.186 (0.30)
CAPEX		5.862* (1.85)	-4.850 (-0.87)
Site_foreign			0.011 (0.05)
Ab_wc_chg		-0.704 (-0.65)	-2.284 (-1.39)
Ab_disexp		0.891** (2.47)	-0.443 (-0.74)
Ab_prod		-1.906** (-2.44)	-3.553*** (-2.65)
Constant	-0.011 (-0.25)	-2.788 (-1.00)	3.900 (0.75)
Observations	2,393	2,099	1,659
R-squared	0.809	0.820	0.195
Fixed effects	Site&Year	Site&Year	Firm&Cat.&Year

Table 7: Cost considerations: Board committee privacy oversight

Table 7 documents the mitigating impacts of board committee privacy oversight on abnormal tracking in suspect firm-years. Columns (1) and (2) present the results with $Ab\_trackers$ as the dependent variable, while Column (3) presents the results with $\Delta Trackers$ as the dependent variable. t-statistics are reported in parenthesis. Appendix A provides variable definitions. Ind. denotes industry and Cat. denotes website category. Two-tailed significance levels are denoted by: *** 1 percent, ** 5 percent, and * 10 percent.

VARIABLES	(1) Ab_trackers	(2) Ab_trackers	(3) $\Delta Trackers$
Suspect × Board_privacy	-2.112**	-2.249**	-4.565***
	(-2.18)	(-2.48)	(-3.61)
Suspect	2.922***	2.955***	4.701***
	(3.63)	(3.95)	(4.51)
Board_privacy	0.511**	0.607**	1.254***
	(2.24)	(2.45)	(2.88)
Size		0.264	-1.221**
		(0.87)	(-2.09)
Lev		1.025**	-1.370**
		(2.55)	(-2.00)
Turnover		-0.640	1.001
		(-1.41)	(1.30)
CAPEX		6.510*	-1.751
		(1.91)	(-0.29)
Site_foreign			0.095
			(0.38)
Ab_wc_chg		-0.117	-2.317
		(-0.09)	(-1.13)
Ab_disexp		1.129**	0.056
		(2.05)	(0.07)
Ab_prod		-1.513*	-3.783**
		(-1.70)	(-2.53)
Constant	-0.451***	-3.869	11.393*
	(-3.02)	(-1.16)	(1.78)
Observations	1,981	1,810	1,440
R-squared	0.809	0.823	0.213
Fixed effects	Site&Year	Site&Year	Firm&Cat.&Year

Table 8: Test of mechanisms

Table 8 presents the results of two mechanism tests. Columns (1) and (2) examine site popularity as a mechanism by which suspect firms meet benchmarks through abnormal tracking, while Columns (3) and (4) investigate discretionary expense effectiveness as the second mechanism. t-statistics are reported in parenthesis. Appendix A provides variable definitions. Ind. denotes industry and Cat. denotes website category. Two-tailed significance levels are denoted by: *** 1 percent, ** 5 percent, and * 10 percent.

VARIABLES	(1) Ab_trackers	(2) $\Delta Trackers$	(3) Ab_trackers	(4) $\Delta Trackers$
Suspect × Popular	1.401**	1.893***		
	(2.55)	(2.81)		
Popular	-0.207	0.157		
	(-1.22)	(1.22)		
Suspect × Disc_effective			1.344***	1.584**
			(2.68)	(2.27)
Disc_effective			-0.013	0.047
			(-0.08)	(0.20)
Suspect	-1.616	-2.592	-0.782	-1.096
	(-1.26)	(-1.62)	(-0.83)	(-0.84)
Size	0.186	-0.577	0.232	-0.457
	(0.72)	(-1.20)	(0.90)	(-0.95)
Lev	0.723**	-0.459	0.810**	-0.346
	(2.21)	(-0.84)	(2.46)	(-0.63)
Turnover	-0.773**	0.180	-0.788**	0.155
	(-2.01)	(0.29)	(-1.97)	(0.24)
CAPEX	6.387**	-4.209	5.803*	-4.540
	(2.01)	(-0.76)	(1.80)	(-0.80)
Site_foreign		0.188		0.011
		(0.72)		(0.05)
Ab_wc_chg	-0.772	-2.222	-0.713	-2.325
	(-0.71)	(-1.35)	(-0.66)	(-1.41)
Ab_disexp	0.810**	-0.573	0.859**	-0.490
	(2.25)	(-0.97)	(2.35)	(-0.81)
Ab_prod	-2.037***	-3.689***	-1.924**	-3.682***
	(-2.61)	(-2.75)	(-2.42)	(-2.71)
Constant	-1.964	5.208	-2.811	4.251
	(-0.70)	(1.00)	(-1.00)	(0.81)
Observations	2,099	1,659	2,099	1,659
R-squared	0.820	0.196	0.820	0.193
Fixed effects	Site&Year	Firm&Cat.&Year	Site&Year	Firm&Cat.&Year

Table 9: Additional Tests: Analyst forecasts as an alternative benchmark

Table 9 presents the results using analysts' forecasts as alternative earnings benchmarks. $Suspect\_ibes$ equals one for firms that exceed the average analyst forecast by two cents or less, based on forecasts issued within 90 days prior to the earnings announcement, and zero otherwise. t-statistics are reported in parenthesis. Appendix A provides variable definitions. Two-tailed significance levels are denoted by: *** 1 percent, ** 5 percent, and * 10 percent.

VARIABLES	(1) Ab_trackers	(2) Ab_trackers	(3) Ab_trackers
Suspect_ibes	0.627**	0.693**	0.555**
	(2.32)	(2.52)	(2.01)
Size		-0.049	0.177
		(-0.17)	(0.61)
Lev		0.860**	0.850**
		(2.37)	(2.24)
Turnover		-0.805**	-1.036**
		(-2.14)	(-2.47)
CAPEX		6.926**	7.114**
		(2.07)	(2.04)
Ab_wc_chg			0.450
			(0.40)
Ab_disexp			0.700*
			(1.86)
Ab_prod			-2.092**
			(-2.52)
Constant	-0.159***	0.078	-2.334
	(-3.49)	(0.03)	(-0.73)
Observations	2,039	2,039	1,906
R-squared	0.807	0.809	0.809
Fixed effects	Site&Year	Site&Year	Site&Year

Table 10: Robustness tests: Alternative method of identifying suspects

Table 10 presents an alternative method of identifying suspects and measuring abnormal tracking. Columns (1) to (3) replicate the findings by using net sales as an alternative deflator for earnings change to identify suspect firms. t-statistics are reported in parenthesis. Appendix A provides variable definitions. Ind. denotes industry and Cat. denotes website category. Two-tailed significance levels are denoted by: *** 1 percent, ** 5 percent, and * 10 percent.

VARIABLES	(1) Ab_trackers	(2) Ab_trackers	(3) Ab_trackers
Suspect_sale	0.917**	1.887***	2.510***
	(2.03)	(2.89)	(2.91)
SASB_material × Suspect_sale		-1.754**	
		(-2.00)	
SASB_privacy		-	
Board_privacy × Suspect_sale			-2.254**
			(-2.23)
Board_privacy			0.594**
			(2.39)
Size		0.203	0.232
		(0.78)	(0.76)
Lev		0.774**	1.005**
		(2.36)	(2.49)
Turnover		-0.871**	-0.763*
		(-2.25)	(-1.68)
CAPEX		5.877*	6.606*
		(1.85)	(1.93)
Ab_wc_chg		-0.535	0.179
		(-0.49)	(0.13)
Ab_disexp		0.942***	1.336**
		(2.60)	(2.42)
Ab_prod		-1.895**	-1.533*
		(-2.41)	(-1.72)
Constant	-0.003	-2.437	-3.387
	(-0.08)	(-0.87)	(-1.02)
Observations	2,391	2,099	1,810
R-squared	0.808	0.819	0.822
Fixed effects	Site&Year	Site&Year	Site&Year

References

Abraham, Rene, Johannes Schneider, and Jan Vom Brocke. 2019. Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management* 49: 424–438.

Amir, Eli, Shai Levi, and Tsafrir Livne. 2018. Do firms underreport information on cyber-attacks? evidence from capital markets. *Review of Accounting Studies* 23: 1177–1206.

Ashraf, Musaib 2022. The role of peer events in corporate governance: Evidence from data breaches. *The Accounting Review* 97(2): 1–24.

Ashraf, Musaib, and Jayanthi Sunder. 2023. Can shareholders benefit from consumer protection disclosure mandates? evidence from data breach disclosure laws. *The Accounting Review* pages 1–32.

Barth, Mary E, John A Elliott, and Mark W Finn. 1999. Market rewards associated with patterns of increasing earnings. *Journal of Accounting Research* 37(2): 387–413.

Barton, Jan, and Paul J Simko. 2002. The balance sheet as an earnings management constraint. *The Accounting Review* 77(s-1): 1–27.

Baruh, Lemi, Ekin Secinti, and Zeynep Cemalcilar. 2017. Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication* 67(1): 26–53.

Borgman, Hans, Hauke Heier, Bouchaib Bahli, and Thomas Boekamp. 2016. Dotting the i and crossing (out) the t in it governance: New challenges for information governance. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* pages 4901–4909. IEEE.

Burgstahler, David, and Ilia Dichev. 1997. Earnings management to avoid earnings decreases and losses. *Journal of Accounting and Economics* 24(1): 99–126.

Caskey, Judson, and N Bugra Ozel. 2017. Earnings expectations and employee safety. *Journal of Accounting and Economics* 63(1): 121–141.

Cohen, Daniel A, Aiyesha Dey, and Thomas Z Lys. 2008. Real and accrual-based earnings management in the pre-and post-sarbanes-oxley periods. *The Accounting Review* 83(3): 757–787.

DeAngelo, Harry, Linda DeAngelo, and Douglas J Skinner. 1996. Reversal of fortune dividend signaling and the disappearance of sustained earnings growth. *Journal of financial Economics* 40(3): 341–371.

Dechow, Patricia M, and Ilia D Dichev. 2002. The quality of accruals and earnings: The role of accrual estimation errors. *The Accounting Review* 77(s-1): 35–59.

Dechow, Patricia M, Richard G Sloan, and Amy P Sweeney. 1995. Detecting earnings management. *Accounting Review* pages 193–225.

Englehardt, Steven, and Arvind Narayanan. 2016. Online tracking: A 1-million-site measurement and analysis. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* pages 1388–1401.

Ford, Roger Allan 2019. Data scams. *Hous. L. Rev.* 57: 111.

García-Sánchez, Isabel-María, Luis Rodríguez-Domínguez, and José-Valeriano Frías-Aceituno. 2015. Board of directors and ethics codes in different corporate governance systems. *Journal of Business Ethics* 131: 681–698.

Goldfarb, Avi, and Catherine E Tucker. 2011. Privacy regulation and online advertising. *Management science* 57(1): 57–71.

Haapamäki, Elina, and Jukka Sihvonen. 2019. Cybersecurity in accounting research. *Managerial Auditing Journal* 34(7): 808–834.

Ham, Charles, Mark Lang, Nicholas Seybert, and Sean Wang. 2017. Cfo narcissism and financial reporting quality. *Journal of Accounting Research* 55(5): 1089–1135.

Healy, Paul M, and James M Wahlen. 1999. A review of the earnings management literature and its implications for standard setting. *Accounting Horizons* 13(4): 365–383.

Huang, Henry He, and Chong Wang. 2021. Do banks price firms' data breaches? *The Accounting Review* 96(3): 261–286.

Ikram, Muhammad, Rahat Masood, Gareth Tyson, Mohamed Ali Kaafar, Noha Loizon, and Roya Ensafi. 2019. The chain of implicit trust: An analysis of the web third-party resources loading. In *The World Wide Web Conference* pages 2851–2857.

Johnson, Garrett 2013. The impact of privacy policy on the auction market for online display advertising.

Johnson, Garrett A, Scott K Shriver, and Shaoyin Du. 2020. Consumer privacy choice in online advertising: Who opts out and at what cost to industry? *Marketing Science* 39(1): 33–51.

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

Jones, Jennifer J 1991. Earnings management during import relief investigations. *Journal of Accounting Research* 29(2): 193–228.

Karaj, Arjaldo, Sam Macbeth, Rémi Berson, and Josep M Pujol. 2018. Whotracks. me: Shedding light on the opaque world of online tracking. *arXiv preprint arXiv:1804.08959*.

Khan, Mozaffar, George Serafeim, and Aaron Yoon. 2016. Corporate sustainability: First evidence on materiality. *The Accounting Review* 91(6): 1697–1724.

Klein, April 2002. Audit committee, board of director characteristics, and earnings management. *Journal of Accounting and Economics* 33(3): 375–400.

Klein, April, Raffaele Manini, and Yanting Shi. 2022. Across the pond: How us firms' boards of directors adapted to the passage of the general data protection regulation. *Contemporary Accounting Research* 39(1): 199–233.

Kothari, Sagar P, Andrew J Leone, and Charles E Wasley. 2005. Performance matched discretionary accrual measures. *Journal of Accounting and Economics* 39(1): 163–197.

Lakonishok, Josef, Andrei Shleifer, and Robert W Vishny. 1994. Contrarian investment, extrapolation, and risk. *The journal of finance* 49(5): 1541–1578.

Larsson, Stefan, Anders Jensen-Urstad, and Fredrik Heintz. 2021. Notified but unaware: Third-party tracking online. *Critical Analysis of Law* 8(1): 101–120.

Lefrere, Vincent, Logan Warberg, Cristobal Cheyre, Veronica Marotta, and Alessandro Acquisti. 2022. Does privacy regulation harm content providers? a longitudinal analysis of the impact of the gdpr. *A Longitudinal Analysis of the Impact of the GDPR (October 5, 2022)*.

Liu, Zheng, Hongtao Shen, Michael Welker, Ning Zhang, and Yang Zhao. 2021. Gone with the wind: An externality of earnings pressure. *Journal of Accounting and Economics* 72(1): 101403.

Lohrke, Franz T, and Cynthia Frownfelter-Lohrke. 2023. Cybersecurity research from a management perspective: A systematic literature review and future research agenda. *Journal of General Management* page 03063070231200512.

Lukic, Karlo, Klaus M Miller, and Bernd Skiera. 2023. The impact of the general data protection regulation (gdpr) on online tracking. *Available at SSRN*.

Manchanda, Puneet, Jean-Pierre Dubé, Khim Yong Goh, and Pradeep K Chintagunta. 2006. The effect of banner advertising on internet purchasing. *Journal of Marketing Research* 43(1): 98–108.

Martin, Kelly D, Abhishek Borah, and Robert W Palmatier. 2017. Data privacy: Effects on customer and firm performance. *Journal of Marketing* 81(1): 36–58.

Mayer, Jonathan R, and John C Mitchell. 2012. Third-party web tracking: Policy and technology. In *2012 IEEE symposium on security and privacy* pages 413–427. IEEE.

McNichols, Maureen F 2002. Discussion of the quality of accruals and earnings: The role of accrual estimation errors. *The Accounting Review* 77(s-1): 61–69.

Myers, James N, Linda A Myers, and Douglas J Skinner. 2007. Earnings momentum and earnings management. *Journal of Accounting, Auditing & Finance* 22(2): 249–284.

Palmatier, Robert W, Kelly D Martin, Robert W Palmatier, and Kelly D Martin. 2019. Big data's marketing applications and customer privacy. *The Intelligent Marketer's Guide to Data Privacy: The Impact of Big Data on Customer Trust* pages 73–92.

Pavlou, Paul A, Huigang Liang, and Yajiong Xue. 2007. Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS quarterly* pages 105–136.

Peukert, Christian, Stefan Bechtold, Michail Batikas, and Tobias Kretschmer. 2022. Regulatory spillovers and data governance: Evidence from the gdpr. *Marketing Science* 41(4): 746–768.

Richardson, Vernon J, Rodney E Smith, and Marcia Weidenmier Watson. 2019. Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems* 33(3): 227–265.

Roychowdhury, Sugata 2006. Earnings management through real activities manipulation. *Journal of Accounting and Economics* 42(3): 335–370.

Sahni, Navdeep S, Sridhar Narayanan, and Kirthi Kalyanam. 2019. An experimental investigation of the effects of retargeted advertising: The role of frequency and timing. *Journal of Marketing Research* 56(3): 401–418.

Urban, Tobias, Martin Degeling, Thorsten Holz, and Norbert Pohlmann. 2020. Beyond the front page: Measuring third party dynamics in the field. In *Proceedings of The Web Conference 2020* pages 1275–1286.

Vorst, Patrick 2016. Real earnings management and long-term operating performance: The role of reversals in discretionary investment cuts. *The Accounting Review* 91(4): 1219–1256.

Yousfi, Karima, and Ojo Johnson Adelakun. 2022. A qualitative approach to google analytics to boost e-commerce sales. In *International Conference on Managing Business Through Web Analytics* pages 73–91. Springer.

Yu, Jongsik, Hyoungeun Moon, Bee-Lia Chua, and Heesup Han. 2022. Hotel data privacy: strategies to reduce customers' emotional violations, privacy concerns, and switching intention. *Journal of Travel & Tourism Marketing* 39(2): 215–227.

Zang, Amy Y 2012. Evidence on the trade-off between real activities manipulation and accrual-based earnings management. *The Accounting Review* 87(2): 675–703.

1.2