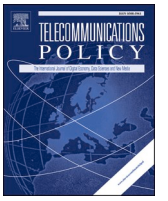
Telecommunications Policy 50 (2026) 103192

Contents lists available at ScienceDirect

Telecommunications Policy

journal homepage: www.elsevier.com/locate/telpol



The impact of platform-level privacy policies on users' privacy concerns: Evidence from Apple App Tracking Transparency via a dynamic difference-in-difference analysis

Sangjun Nam [a,b,*], Youngsun Kwon [a]

[a] School of Business and Technology Management, College of Business, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon, 34141, Republic of Korea
[b] Technology Policy Research Division, Electronics and Telecommunications Research Institute, 218 Gajeong-ro, Yuseong-gu, Daejeon, 34129, Republic of Korea

ARTICLE INFO

Keywords:
Personal data
Online platform
Regulation
Privacy Concern
App Tracking Transparency
Korean Media Panel survey

ABSTRACT

Apple App Tracking Transparency (Apple ATT), one of the representative platform-level privacy policies, was introduced in April 2021. Considering that privacy concerns can affect users' privacy behavior as an antecedent, it is meaningful to investigate the impact of Apple ATT on users' privacy concerns to explore the effect of platform-level privacy policies on the digital society as well as their own platform ecosystems. However, there exist mixed views that the Apple ATT can either strengthen or mitigate users' privacy concerns by increasing privacy awareness or trustworthiness. In addition, the frame of the Apple ATT prompt may negatively affect users' perceptions of information privacy. To investigate which effect is stronger than the other, this study implemented a dynamic Difference-in-Difference analysis in a quasi-experimental setting. The result showed that introducing Apple ATT strengthened users' privacy concerns in the short term. It implies that platform-level privacy policies may shape users' privacy perceptions by increasing privacy concerns. Moreover, this strengthened effect on privacy concerns due to the Apple ATT could be moderated by privacy protection literacy.

1. Introduction

Collecting users' personal data is common in exchange for various purposes on online platforms, and the personal data is used for monetizing and attracting more users. Therefore, online platforms have an incentive to collect personal data from users excessively (Stucke & Ezrachi, 2016; Stucke, 2018). These online platforms' personal data practices may lead to negative perceptions among users, including privacy concerns (Boerman et al., 2017; Tucker, 2012; Moore et al., 2015). Against this background, enhanced personal data protection regulations began to be introduced, starting with the European Union's (EU's) General Data Protection Regulation (GDPR), perceived as the gold standard on personal data protection regulations (Ke & Sudhir, 2023). These regulations aim to protect users' information privacy and relieve negative perceptions related to personal data collections by prohibiting firms from excessively using and utilizing personal data without sufficient notice and consent.

In this regulatory environment, Google and Apple have announced and introduced their own personal data protection policy such

* Corresponding author. Technology Policy Research Division, Electronics and Telecommunications Research Institute, 218 Gajeong-ro, Yuseong-gu, Daejeon, 34129, Republic of Korea.
E-mail addresses: sjnam@etri.re.kr (S. Nam), yokwon@kaist.ac.kr (Y. Kwon).

https://doi.org/10.1016/j.telpol.2026.103192
Received 16 November 2025; Received in revised form 11 March 2026; Accepted 12 March 2026
Available online 18 March 2026

as Apple App Tracking Transparency (Apple ATT[1]) and Google Privacy Sandbox as a de facto privacy regulator for protecting their users' information privacy as well as complying the regulations (Geradin et al., 2021; Kollnig et al., 2022; Van Hoboken & Fathaigh, 2021). Gatekeeper platforms could gain an advantage by making it difficult for third parties to collect users' personal data (Geradin et al., 2021; Kramer, 2025), as well as by creating an image of themselves as committed to protecting information privacy. In line with this context, previous studies have focused on the effect of gatekeepers' privacy policies on platform ecosystems or competitors from various perspectives (Baviskar et al., 2024; Cheyre et al., 2023; Geradin et al., 2021; Kollnig et al., 2022; Krämer, 2025). However, there is a lack of discussion on the indirect effect of those privacy policies on digital society, as they change users' privacy perceptions. The introduction of gatekeepers' privacy policy could affect their billions of users' privacy perceptions, such as privacy concerns and trustworthiness about data collectors, which may increase or decrease data collectors' capabilities of collecting personal data by encouraging or discouraging users' willingness to share personal data (Bélanger & Crossler, 2011; Smith et al., 2011). Therefore, it can be said that it is also meaningful to investigate how gatekeepers' privacy policies affect users' privacy perceptions.

However, it is uncertain the effect of introducing gatekeeper platforms' privacy policies on users' privacy concerns because new policies could generate two seemingly conflicting effects, such as relieving users' privacy concerns by improving the trustworthiness related to data collectors (Bauer et al., 2022; Fox et al., 2022; Wu et al., 2012) or increasing users' privacy concerns by awakening privacy awareness (Benamati et al., 2017; Bergmann, 2008; Schaub et al., 2016). Moreover, considering that gatekeeper platforms could have different incentives, as previous studies noted, the effect of privacy policies in gatekeeper platforms on users' privacy concerns could differ from national-level privacy regulations, even though they act as a de facto regulator based on the 'platforms of platforms' characteristic. Considering that the effect of privacy interventions on users' privacy perceptions can vary across depending on the contents of interventions as well as individual characteristics and situational contexts (Dinev et al., 2015), the effect of gatekeeper platforms' personal data protection regulation on users' privacy concerns is still in a gray area, given these mixed views and distinct characteristics of gatekeeper platforms, requiring further in-depth studies. Observing these research needs, this paper aims to shed light on the effect of gatekeeper platforms' personal data protection regulation on users' privacy concerns. Empirical evidence on the effects of gatekeepers' privacy policies could have meaningful implications for regulators and data-driven businesses in balancing the protection of users' personal data with the efficient use of that data.

To investigate the causal effect of gatekeepers' privacy policies on users' privacy concerns, we focus on the short-term effect of introducing Apple ATT, a representative gatekeeper platform-level privacy policy, on users' privacy concerns using Difference-in-Differences (DID) estimation in a quasi-experimental setting. One general approach to investigating the causal effect of policies is estimating the average effect of exposure to the policies on eligible units with the DID estimation. In this study, iOS users and non-iOS users can be classified into the treatment and control groups, respectively, focusing on estimating the intention-to-treat (ITT) effects of the introduction of Apple ATT, given that the actual exposure of Apple ATT may vary across iOS users based on smartphone usage patterns and update behavior. We also focus on the short-term effect because it is not easy to control external factors[2] that can affect users' privacy perceptions over a longer period in the quasi-experiment setting. In this approach, our findings offer a distinct perspective by estimating the changes in users' privacy concerns before and after the introduction of Apple ATT using a quasi-experimental design based on secondary data, rather than relying on laboratory experiments or direct surveys.

The remainder of this paper is organized as follows. Section 2 reviews previous studies on the concept of Apple ATT as a gatekeeper platform's privacy policy. It also reviews the concept of information privacy and information privacy concerns, and previous studies that investigated the relationship between privacy governance interventions and information privacy concerns, and the gatekeepers' privacy policy. Section 3 presents this study's research methodology and data. Section 4 reports and interprets the empirical findings. Finally, Section 5 discusses the implications.

2. Literature review

2.1. Apple App Tracking Transparency as a gatekeeper platform's privacy policy

Smartphone platforms, one of the representative gatekeeper platforms, are perceived as 'platforms of platforms' on other platforms (Nooren et al., 2018). Van Hoboken and Fathaigh (2021) explained that these platforms act as regulators based on the intermediate function accompanied by a rule-setting feature. In line with this context, they argued that the smartphone platforms that find themselves in a role as privacy regulators are introducing platform-level privacy regulations. In April 2021, Apple introduced the Apple ATT, requiring iOS apps to ask users for explicit permission before tracking. Under the Apple ATT, the app can access the Identifier for Advertisers (IDFA), a random and unique identifier provided by the operating systems (OS) to apps for tracking users in the OS, only if an iOS users consent to track (Kollnig et al., 2022).

Even though the Apple ATT was introduced to ensure users' choice rights related to information privacy, the effect of Apple ATT on

[1] To distinguish Apple App Tracking Transparency from ATT, the abbreviation for average treatment effects on the treated group, we used Apple ATT as the abbreviation for App Tracking Transparency.

[2] After the Apple ATT was introduced, Google also announced the Privacy Sandbox on Android in February 2022, similar to the Apple ATT. However, they mentioned that they plan to support existing platform features for at least two years while design, build, and test new solutions (Google Blog, https://blog.google/products/android/introducing-privacy-sandbox-android/). It means that there was no smartphone OS-level privacy policy implementation on Android similar to the Apple ATT until at least 2024. However, there could be still another platform-level polices and events related to personal data collection that affect users' privacy perceptions after the Apple ATT was introduced.

the iOS platform ecosystem, especially on third-party app providers, has been controversial. Some previous literature argued that different strategies of Apple ATT between iOS native apps and third-party apps can be used for gaining a dominant position in terms of personal data on their platform (Baviskar et al., 2024; Cheyre et al., 2023; Geradin et al., 2021; Kollnig et al., 2022; Krämer, 2025). From another perspective, Apple ATT may also affect iOS users' perceptions of information privacy (Baviskar et al., 2024), and these changes in users' perceptions could influence their information privacy behavior across other digital platforms as well as iOS. However, to the best of our knowledge, there is a lack of studies exploring the relationship between Apple ATT and users' information privacy concerns, given these distinct characteristics, which is one of the important antecedents of information privacy decision and behavior. To help fill this gap, this paper aims to investigate the relationship between the introduction of Apple ATT, a well-known gatekeeper-level privacy policy, and users' privacy concerns. To discuss the relationship between Apple and privacy concerns, we began by exploring the concept of information privacy and its importance in the context of personal data collection on digital platforms in the next section.

2.2. The concept of information privacy and information privacy concerns

Information privacy, a subset of whole privacy concepts, concerns access to individually identifiable personal data (Smith et al., 2011). From this perspective, many researchers have noted that information privacy is related to controlling personal data collection and use (Bélanger & Crossler, 2011; Hann et al., 2007; Stone & Stone, 1990). Therefore, it can be viewed that users worry about personal data collection on online platforms in terms of information privacy.[3] This individual's concern regarding their information privacy refers to information privacy concerns (Smith et al., 1996). Dinev and Hart (2006) described that privacy concerns are beliefs about who has access to their disclosed personal information via the internet and how it is utilized. Thus, privacy concerns are increased due to the uncertainty of access and use of personal data (Dinev & Hart, 2006). In summary, users' perceptions related to collecting and utilizing personal data on digital platforms can be measured by information privacy concerns (Smith et al., 2011).

Information privacy concerns are one of the key concepts explaining the users' information privacy behaviors (Bélanger & Crossler, 2011; Smith et al., 2011). Previous findings suggest that information privacy concerns influence individuals' privacy attitudes as well as acceptance of technology and services in various contexts (Dienlin & Metzger, 2016; Dinev & Hart, 2006; Fox et al., 2021; Malhotra et al., 2004; Van Slyke et al., 2006). This implies that the high level of information privacy concerns has a negative impact on the data-driven industry by discouraging users' acceptance of data-based services and their willingness to share personal data. Therefore, it is important to investigate the impact of Apple ATT on users' information privacy concerns for understanding the effect of gatekeeper platforms' privacy policies on data-based businesses as well as on their platform ecosystem.

2.3. The privacy regulations and information privacy concerns

In the previous section, we briefly reviewed the characteristics of the Apple ATT as a gatekeeper platform-level privacy policy, and explored why information privacy concerns are an important concept in the context of personal data collection in digital society. In this section, we reviewed previous literature on the relationship between privacy regulations and information privacy concerns, including studies on service-level privacy policies, and derived hypotheses about the short-term effect of Apple ATT on users' privacy concerns. However, rather than directly identifying and testing the specific mechanisms via measuring various users' privacy perceptions, such as trustworthiness and awareness, along with privacy concerns, this study focuses on quasi-experimentally estimating the short-term direction of observed changes in privacy concerns following the introduction of Apple ATT. Accordingly, the mechanisms discussed below are used to motivate this study's hypotheses about the short-term direction of changes in privacy concerns following the Apple ATT and are positioned not as a definitive causal explanation but as a literature-informed interpretive framework for interpreting the empirical findings.

Privacy regulations typically encompass information disclosure related to personal data practices as well as policy-related signals that affect users' perceptions. Previous studies suggested that privacy policies and privacy seals can be perceived not only as detailed information but also as heuristic cues that signal trustworthiness, particularly when users do not care about the details of the policy (LaRose & Rifon, 2006; Rifon et al., 2005; Wang et al., 2004). In particular, Earp and Baumer (2003) noted that most internet users appear to be reassured by the presence of a privacy policy even though they do not scrutinize policy details. This suggests that the mere presence of a privacy policy may serve as an assurance cue. In line with this context, several studies investigated the relationship between the online privacy policy and privacy perceptions/behaviors (Jensen et al., 2005; Wu et al., 2012; Xu et al., 2011). Xu et al. (2011) showed that privacy regulations as institutional privacy assurances mitigate privacy concerns by increasing perceived privacy control, which can be changed by users' perceived effectiveness of privacy policy. Wu et al. (2012) found that the five dimensions of privacy policy, such as notice, choice, access, security, and enforcement, mitigate privacy concerns, and some of these dimensions have a positive relationship with trust. Similarly, Jensen et al. (2005) noted that the mere presence of privacy policies, rather than their content, functions as a "trust-mark" that affects users positively.

Regulatory frameworks can also affect users' privacy perceptions positively in terms of the assurance aspect by ensuring rights of control and choice over the access and use of personal data. For example, the GDPR aims to clarify, codify, and extend individual data rights (Bauer et al., 2022). In a similar vein, the Personal Data Protection Act has been devised to ensure notification consent before

[3] We did not strictly distinct two terms privacy and information privacy throughout the remainder of this paper because the privacy term also used as an information privacy context in many previous studies.

collecting and utilizing users' personal data in South Korea. Building on these institutional features, Bauer et al. (2022) discussed that the awareness of GDPR positively affects users' trust in data collectors because they can expect that data collectors will not misuse their data to comply with the GDPR. Fox et al. (2022) also found that the GDPR label affects users' trustworthiness positively. Considering the negative relationship between privacy concerns and trust (Bélanger & Crossler, 2011; Smith et al., 2011; Swani et al., 2021), the privacy regulation may mitigate users' privacy concerns by enhancing trust. However, Bauer et al. (2022) also noted that the mere implementation of privacy regulations may be insufficient to increase users' trust in data collectors. It implies that the effect of privacy regulations may vary across users and contexts, depending on individuals' characteristics and situational factors.

On the other hand, personal data protection regulations may strengthen users' information privacy concerns by increasing privacy awareness. Privacy awareness refers to the degree to which individuals are aware of organizations' privacy practices (Ozdemir et al., 2017; Smith et al., 2011). Under the "Antecedents – Privacy Concerns – Outcomes" (APCO) framework, which Smith et al. (2011) suggested, privacy awareness could increase privacy concerns as an antecedent (Benemati et al., 2017; Ozdemir et al., 2017). Previous studies also noted that the awareness of online platform practices, which involve collecting, using, and sharing behavioral data, could raise privacy concerns (Boerman et al., 2017; Tucker, 2012). Users' privacy awareness can be enhanced due to the personal data protection regulation by providing knowledge related to the practices of collecting and utilizing personal data. For example, in South Korea, firms that collect and use personal data should periodically report the information related to personal data to each user in accordance with the Personal Information Protection Act (PIPA). This report includes various information related to personal data practices, and it reminds users that firms collect and use users' personal data for their own purposes. In this view, Bergmann (2008) found a positive relationship between privacy policy and privacy awareness. Similar to the privacy policy at the service level, Fox et al. (2022) found that the GDPR privacy label affects users' perceptions of privacy. In line with these previous findings, Schaub et al. (2016) empirically showed that the new awareness of the prevalence of tracking gained through the browser extension that provides information about the tracking of personal data could increase users' privacy concerns. Notably, disclosures and privacy notices are not always processed as deliberative informational input, as mentioned before. Instead, these notices may function as salient cues that make users easily aware of potential privacy risks (John et al., 2011; Singer et al., 1992). John et al. (2011) found that formal privacy notices can influence participants' willingness to divulge sensitive information. It suggested that formal privacy notices can backfire by arousing privacy concerns. Ebert et al. (2021) also showed that privacy notices increase privacy awareness when exposed in a salient manner, with effects that vary by the levels of riskiness of the privacy notices. In summary, these studies support the possibility that privacy interventions may strengthen privacy concerns by increasing the salience of data practices and updating users' awareness of privacy risks.

Previous findings suggest that the personal data protection regulation could generate two mixed effects: easing privacy concerns by improving trustworthiness or strengthening users' privacy concerns by elevating awareness and salience of data practices. Drawing on the enhanced APCO model proposed by Dinev et al. (2015), these seemingly conflicting findings in the previous literature can be reconciled. Unlike the original APCO model, the enhanced APCO model emphasizes that privacy-related attitudes and behaviors are shaped by low-effort cognitive processing as well as deliberative (high-effort) cognitive processing. It suggests that behavioral factors such as limited cognitive resources and heuristics may affect privacy-related attitudes and behaviors. From this perspective, the effect of privacy regulations on users' privacy perceptions may vary across users and contexts, depending on individual characteristics and situational conditions.

These conflicting effects also apply to Apple ATT in a similar way. Depending on users' interpretations, the introduction of Apple ATT may either increase users' trust in iOS's personal data practices by implying that the platform pays attention to their information privacy, as Apple (2021) noted, or awaken iOS users' awareness of the prevalence of data tracking, which requires platform intervention. In addition, Apple ATT could either increase users' trust in its handling of third-party apps' data tracking or increase users' privacy awareness through Apple ATT-related notice for iOS users that each third-party app is tracking personal data. In particular, the Apple ATT prompt, when encountered, may serve as a salient privacy notice that makes potential privacy risks cognitively accessible. In this regard, its message framing, which may reflect Apple's differential stance toward third-party tracking, may shift users' privacy-related perceptions in a negative direction (Baviskar et al., 2024; Dinev et al., 2015; Ebert et al., 2021).

To derive hypotheses about the short-term effect of Apple ATT on users' privacy concerns, we adopt Dinev et al. (2015), who suggest that users may engage in low-effort cognitive processing regarding data collection and tracking practices in the casual mobile context. Indeed, survey results showed that the majority of users tend to rely on "unconscious consent" when faced with terms and conditions regarding personal data collection (Pew Research Center, 2019; PIPC & KISA, 2023). It implies that most users may not perceive personal data collection practices precisely without any additional notice because they consent to personal data collection unconsciously. In that case, the introduction of Apple ATT may make users more likely to move from a low-effort cognitive state to a high-effort one as a salience cue, suggesting that users' abstract tracking practices become cognitively accessible. In this context, this possibility may also be consistent with users' perceived privacy risks becoming aligned with the actual practices. In addition, considering the negativity bias, which refers to a person's tendency to weigh negative information rather than positive information (Ito et al., 1998; Rozin & Royzman, 2001), the effect of privacy awareness, which reminds potential privacy risks (negative information), may be more likely to shape observed short-term changes in privacy concerns than the effect of trustworthiness derived from assurance and transparency (positive information). Moreover, users' trustworthiness in data collectors may not be changed significantly in the short term, as Bauer et al. (2022) found. The authors noted that personal data protection regulations may have a long-term effect. For example, users may take time to sufficiently understand the actual meaning and stipulation of the personal data protection regulations. In this background, we expect that the Apple ATT will increase privacy concerns among iOS users in the short run.

H1. The introduction of Apple App Tracking Transparency increases users' privacy concerns in the short term.

Given that Apple ATT's effect on users' privacy concerns may operate in part through changes in privacy awareness, knowledge of information privacy may be an important factor shaping heterogeneous responses to the Apple ATT. Users with sufficient knowledge of information privacy may not be surprised when new information about data collectors' personal data practices is provided, as they most likely already understand privacy issues. In this context, previous studies found that users with a high level of privacy knowledge hold more stable opinions on privacy issues (Baek, 2014; Park, 2013). By extending this context, grounded in Protection Motivation Theory (PMT), we examined the relationship between privacy-related knowledge and changes in users' privacy perceptions following the Apple ATT, which may serve as a risk-related cue. From the perspective of PMT, individuals adopt protective reactions by evaluating risk messages based on threat and coping appraisals (Maddux & Rogers, 1983; Rogers, 1975). In this regard, self-efficacy, a sub-dimension of coping appraisals, may moderate the impact of salient risk cues on privacy perceptions and protective reactions in the information privacy context (Johnston & Warkentin, 2010; LaRose & Rifon, 2007). In this study, we focus on the knowledge and skills related to privacy and data protection as one key dimension of privacy literacy (Masur, 2020; Trepte et al., 2014). To the extent that such literacy strengthens users' coping appraisal, users who perceive that they have enough knowledge to cope with privacy risks may react less negatively than those who do not when they recognize the prompt/existence of Apple ATT. Therefore, we expect that Apple ATT's effect on users' privacy concerns will vary with the level of privacy knowledge.

H2. The effect of Apple App Tracking Transparency on users' privacy concerns is moderated by privacy protection literacy.

3. Methodology and data

3.1. Dynamic difference-in-difference with CSDID approach

This study uses the dynamic difference-in-difference (dynamic DID) approach, the so-called event study analysis, to investigate the causal effect of the Apple ATT on iOS users' information privacy concerns as Eq. (1). The dynamic DID approach can be helpful in estimating dynamic treatment effects, such as the treatment effect in one year and two years, following the enactment of national law. In this analysis, we use dynamic DID to estimate the short-term causal effect of Apple ATT.

$$IPC_{i,t} = \alpha_i + \lambda_t + \sum_{\ell} \mu_{\ell} I\{t - E_i = \ell\} + \beta^T controls_{i,t} + \varepsilon_{i,t} \quad (1)$$

where $IPC_{i,t}$ is the information privacy concerns for individual i at time t; α_i and λ_t are individual and time fixed effects, respectively; and E_i is the time when the Apple ATT is implemented. $\ell = t - E_i$ denotes the relative period since the Apple ATT was implemented, and $I\{A\}$ denotes the indicator function is the 1 when the A is true.

The DID approaches in the quasi-experimental setting suffer from selection bias. In this study, individuals who consistently prefer and choose the iPhone over other smartphones may have distinct characteristics that could affect their privacy perceptions. To mitigate these selection bias problems, we adopt the CSDID method (Callaway & Sant'Anna, 2021), which uses the Doubly Robust (DR) approach that combines the outcome regression (OR) and inverse probability weighting (IPW) approach proposed by Sant'Anna and Zhao (2020).

3.2. Data: Korean Media Panel Survey

To implement the dynamic DID, we use the Korean Media Panel Survey data from the Korea Information Society Development Institute (KISDI) that have been collected annually since 2010. These datasets are useful for this study because they contain measures of privacy concerns, smartphone devices, digital capabilities related to protecting privacy, and demographic characteristics. The post-treatment period is set after April 2021, based on the introduction of Apple ATT in South Korea with the iOS update. The data period is from 2016.6 to 2021.6, as the KISDI Media Panel Survey is conducted every June, as shown in Fig. 1. KISDI Media Panel Survey has around 10,000 respondents per period, and 4687 respondents have consistently responded to surveys and used smartphones since 2016. iOS users exposed to the Apple ATT are in the treatment group, and those not exposed are in the control group. More specifically, we label people who continuously used an iPhone between 2020.6 and 2021.6 as the treatment group, and respondents who did not use an iPhone during this period as the control group, to capture the short-term causal effect of Apple ATT. However, actual exposure,

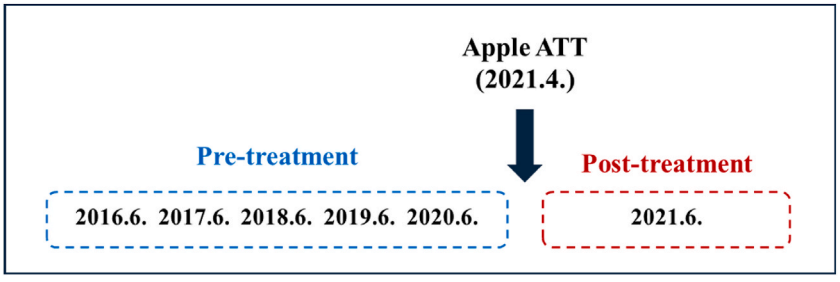


Fig. 1. Data period.

most notably exposure to the Apple ATT prompt, may vary across iOS users based on smartphone usage patterns and update behavior. While we acknowledge this individual heterogeneity in exposure intensity, our study aims to estimate the intention-to-treat (ITT) effect of Apple ATT rather than identifying the average treatment effect of Apple ATT on treated users. Accordingly, we define the treatment as being subject to the Apple ATT policy, rather than directly observed prompt exposure at the individual level. As previous literature noted (Angrist & Pischke, 2009; Ksoll et al., 2016), the ITT effect estimation can be diluted due to imperfect compliance (i.e. delayed or no iOS update), implying that our DID-based ITT effect estimates are likely to be attenuated relative to the effect under full exposure. Considering that imperfect compliance is common in the real-world policy implementation, estimating ITT effects may be a reasonable approach to capturing the average effect of platform-level policy under real-world conditions. Additionally, to mitigate confounding from other external factors, we focus on the short-term effect of Apple ATT. We also dropped samples of those born before 1960 or in 2001 or later who did not use online services continuously during the data period. Finally, the treatment group consists of 174 respondents, and the control group consists of 2925 respondents. Given that the survey data are nationally representative official statistics, we considered the treatment group as likely to represent general iPhone users rather than a specific subgroup, despite its small size.

We consider individual characteristics that could affect users' privacy concerns as antecedents of privacy concerns in the APCO framework (Smith et al., 2011) to verify that the difference in privacy concerns between the treatment group and control group is due to the introduction of Apple ATT. We take into account six individual characteristics: age, gender, digital capabilities related to protecting information privacy (Literacy), highest education level (Edu), monthly income, and monthly payments of mobile services and devices (Exp). Previous studies showed that demographic characteristics are associated with privacy concerns (Benamati et al., 2017; Smith et al., 2011). We selected respondents' self-reported privacy-protective digital capabilities, including awareness of protective measures and coping practices, as a proxy for the knowledge and skills dimension of privacy literacy (Masur, 2020; Park, 2013; Rosenthal et al., 2020; Trepte et al., 2014). This literacy variable may shape information privacy concerns as an antecedent and may also moderate how users appraise and respond to the Apple ATT-related cues. Lastly, the monthly payments for mobile services and devices are also included in the analysis as a proxy for smartphone and mobile service usage. We assumed that smartphone and mobile service use could be related to personal privacy experience, which in turn affects privacy concerns (Benamati et al., 2017; Ozdemir et al., 2017). We also consider the residential area, which is related to social distancing during COVID-19. Kim et al. (2024) found that social distancing during COVID-19 led to a decrease in privacy concerns. Given that Apple ATT was introduced during COVID-19, it needs to be addressed. Following the previous study's estimation strategy of social distancing, we classified the respondents' residential area into Seoul/Gyeonggi-do and other areas. These seven individual characteristics are used in the DR approach. The measurement of individual characteristics is summarized in Table 1.

Information privacy concerns, our primary dependent variable in this analysis, are measured using two items on a 5-point Likert scale in the Korea Media Panel Survey data. There are eight items related to privacy concerns that can be measured continuously from 2016 to 2021 in the Korea Media Panel Survey data; however, we chose two of the eight items that were highly relevant to information privacy concerns in the main analysis. The eight questions related to privacy concerns are summarized in Table 2. Based on the exploratory factor analysis summarized in Table 3, we found that all eight items demonstrated high internal consistency (Cronbach's $\alpha = 0.94$) and loaded onto a single factor. However, the whole eight items encompass conceptually distinct dimensions, such as security threats related to unauthorized secondary use and improper access (Q1, 5, 8) and digital residue (Q2, 3), from information privacy context regarding data collection practices (Bélanger et al., 2002; Malhotra et al., 2004; Smith et al., 2004). To enhance content validity and alignment with our research context, we chose the fourth and sixth items as the measure of information privacy concerns

Table 1
Description of covariates.

Covariates	Measurement
Literacy (5 Likert scale)	Q1. The degree of awareness about the measure of protecting personal data and privacy on the internet. Q2. The degree of awareness about the measure of coping methods when personal data leakage occurs. Q3. The degree of extent of the detection and remedy of malware in smart devices. Q4. The degree of awareness about the measure of classification and **blocking** dangerous text messages such as spam text messages and phishing text messages. Q5. The degree of awareness about the measure of classification and **reporting** dangerous text messages such as spam text messages and phishing text messages.
Gender	Male: 1, Female: 2
Age	Age.
Edu	The highest education level is classified into six levels. We classified these six levels into three: middle school or below, high school, and college or above.
Residential area	Respondents' residential area is classified into seventeen areas. We classified these seventeen areas into two groups: those living in the Seoul/Gyeonggi-do area and other areas during 2020-2021.
Income	Monthly income is classified into eight levels. (No income, less than 500,000 KRW, 500,000 ~ 1,000,000 KRW, 1,000,000 ~ 2,000,000 KRW, …. more than 5,000,000 KRW)
Exp	Monthly payments of mobile services and devices (thousands KRW/month).

Note. The five items related to the literacy variable are measured in only 2020 - 2021, not the whole period, and we used the average value of the Likert scale score in 2020 - 2021 as a time-invariant individual characteristic. These questions, originally written in Korean, were translated into English by the authors.

Table 2
Questionnaires for privacy concerns.

Questionnaire
Q1. I am concerned that someone may gain my personal information.
Q2. I am concerned that my personal information remained in devices that I used before.
Q3. I am concerned that personal information I do not remember may have remained online.
Q4. I am concerned that online sites ask for too much personal information when signing up.
Q5. I am concerned about the unauthorized use of my online ID.
Q6. I am generally concerned about my privacy when using the internet.
Q7. People who do not reveal who they are online are suspicious.
Q8. I am concerned that my personal information, such as my pictures and name, can be misused.

Note. The questionnaires for privacy concerns, originally written in Korean, were translated into English by the authors.

Table 3
Exploratory factor analysis of privacy concerns items.

Items (Short label)	Factor loading	Uniqueness
Q1. Concern that someone may gain personal information	0.8510	0.2758
Q2. Concern about personal info remaining on used devices	0.8426	0.2901
Q3. Concern about personal info remaining online	0.8421	0.2909
Q4. Concern sites ask for too much info at sign-up	**0.8244**	**0.3204**
Q5. Concern about unauthorized use of online ID	0.8452	0.2857
Q6. General privacy concern when using the internet	**0.8522**	**0.2738**
Q7. Suspicious of people who do not reveal their identity online	0.8296	0.3118
Q8. Concern about misuse of pictures/name	0.8836	0.2193
Eigenvalue	5.7322	
Variance Explained (%)	71.65	
Cronbach's α	0.9433	

Note. Unrotated one-factor solution; extraction method = PCF (principal-component factors); N = 18,594.

related to personal data collection online. We viewed that Q4 item measures the concerns about excessive data collection consistent with the 'Collection' dimension, and Q6 item measures general privacy anxiety reflecting 'General Information Privacy Concern' (Malhotra et al., 2004; Smith et al., 1996). To ensure the robustness of our findings, we use the average Likert scale score for two items (IPC) and the average Likert scale score for all eight items (PC) in the main analysis. The statistics of dependent variables and individual characteristics as covariates are summarized in Table 4.

4. Results

4.1. Main results of dynamic difference-in-difference

We first visually examine the trends in privacy concerns, as shown in Fig. 2. The figure shows that the privacy concerns between the treated and control groups were close to each other in the last five years before Apple ATT was introduced. However, after introducing Apple ATT, the privacy concerns between the two groups shifted in opposite directions in the short term. The privacy concerns of the treated group were increased, whereas those of the control group were decreased. We qualitatively examine whether this pronounced decline pattern in the control group reflects Android-side developments and events of comparable salience in the post-treatment period by comparing news trends related to personal data, privacy, and security across two mobile ecosystems. As shown in Appendix Figure A1, we do not observe distinct patterns that stand out relative to prior fluctuations. While news-frequency trends do not provide causality directly, this evidence may help mitigate the alternative explanation that Android-specific events account for the observed group differences. In this context, one plausible interpretation is that this differential pattern may be consistent with the combined influence of common external factors during the COVID-19 period and the introduction of Apple ATT. During COVID-19, social distancing accelerated the adoption and usage of digital services and required users to consent to data tracking for various purposes. Consequently, these recurrent experiences could lead to users' relaxation of their privacy vigilance by habituating these situations (Kim et al., 2024; Wu et al., 2023). In contrast, after the introduction of Apple ATT, iOS users became subject to the possibility of encountering Apple ATT prompt, which alerts them to the tracking of their personal data, and this salient notice may have attenuated such habituation. Nevertheless, concerns may still remain that the DID estimate captures the divergent trend between the two groups rather than the ITT effect of Apple ATT because of the decline observed in the control group. We therefore address this concern explicitly in the subsequent robustness analysis (Section 4.3.1)

Table 4
Summary statistics for the dependent variable and covariates (based on 2020).

	Variable	Mean	SD	Min	Max
Treatment (n = 174)	Privacy concerns				
	Selected two items (IPC)	3.8132	1.0471	1	5
	All items (PC)	3.8326	0.9669	1	5
	Literacy	4.1649	0.8743	1.3	5
	Male	0.3333	0.4728	0	1
	Age	29.6264	9.3798	19	58
	Residential area				
	Seoul/Gyeonggi-do	0.4310	0.4967	0	1
	Others	0.5690	0.4967	0	1
	Education level				
	High school	0.1437	0.3518	0	1
	College or above	0.8563	0.3518	0	1
	Monthly income	3.4943	2.0953	1	8
	Exp	69.4483	36.1649	22	225
Control (n = 2925)	Privacy concerns				
	Selected two items (IPC)	3.7362	0.9166	1	5
	All items (PC)	3.7578	0.8485	1	5
	Literacy	3.3353	1.0527	1	5
	Male	0.4585	0.4984	0	1
	Age	44.5080	11.0272	19	60
	Residential area				
	Seoul/Gyeonggi-do	0.3484	0.4765	0	1
	Others	0.6503	0.4770	0	1
	Moving*	0.0014	0.0370	0	1
	Education level				
	Middle school or below	0.0236	0.1518	0	1
	High school	0.4113	0.4922	0	1
	College or above	0.5651	0.4958	0	1
	Monthly income	3.9744	2.1399	1	8
	Exp	61.5491	23.8196	5	265

Note. *Moving* variable at the *Residential area* means respondents who moved from the Seoul/Gyeonggi-do area to Others during 2020 – 2021, or vice versa.

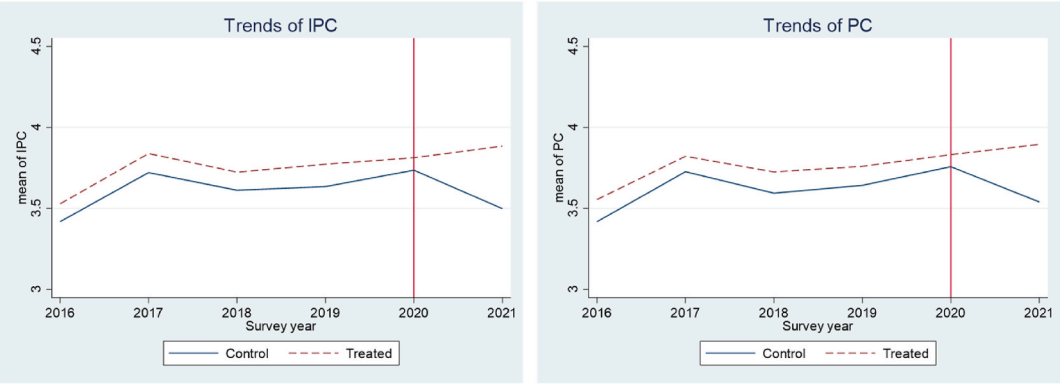


Fig. 2. Trends of privacy concerns between the treated and control groups.

The results of dynamic DID are summarized in Table 5, and the trends in the ITT effect are described in Fig. 3. We used user-written Stata code, *csdid* (Rios-Avila et al., 2023), to implement the dynamic DID using the CSDID approach. Model 1 is the dynamic DID with the dependent variable based on two selected items related to privacy concerns, as explained in the previous section, and Model 2 is with the dependent variable based on all eight items. Before presenting the main estimates, we conduct a set of diagnostic checks given the relatively small treated sample size. Specifically, we check the common support, weight stability, and covariate balance at baseline (2020, the last pre-treatment year) with the propensity score and IPW weights from *drdid* (Rios-Avila et al., 2022), which shares the same DR framework because *csdid* does not report propensity scores and weights directly. Under the definition that the common support region is the intersection of the treated and control groups' propensity score range, 98.3% of treated samples lie within the common support region (see Appendix Tables A1 and A2), suggesting that extrapolation concerns are likely limited. We also evaluate the stability of the weights. In the control group, the maximum IPW weight is 0.987, the 99th percentile is 0.559, and the top 1% of

Table 5
The results of dynamic DID with the CSDID method.

Event time (t)	(1)			(2)		
	Coeff (Std. err)	95% CI	p-value	Coeff (Std. err)	95% CI	p-value
Pre (t = −5)	0.0198 (0.1099)	[-0.1956 0.2351]	0.8571	0.0480 (0.0983)	[-0.1448 0.2407]	0.6257
Pre (t = −4)	0.0251 (0.0922)	[-0.1556 0.2058]	0.7852	−0.0157 (0.0861)	[-0.1845 0.1530]	0.8552
Pre (t = −3)	−0.0190 (0.1031)	[-0.2210 0.1830]	0.8539	−0.0034 (0.0946)	[-0.1887 0.1820]	0.9717
Pre (t = −2)	0.0298 (0.0882)	[-0.1431 0.2027]	0.7353	−0.0156 (0.0794)	[-0.1712 0.1400]	0.8446
Post (t = 0)	0.2251** (0.0995)	[0.0301 0.4200]	0.0236	0.1941** (0.0906)	[0.0166 0.3715]	0.0321
Pre-average	0.0139 (0.0807)	[-0.1442 0.1721]	0.8628	0.0033 (0.0745)	[-0.1428 0.1494]	0.9643
Post-average	0.2251** (0.0995)	[0.0301 0.4200]	0.0236	0.1941** (0.0906)	[0.0166 0.3715]	0.0321
Obs.	18,594			18,594		
Pre-trend test (p-value)	0.9830			0.9445		
Covariates	Yes			Yes		
Individual FE	Yes			Yes		
Year FE	Yes			Yes		

Note. *** significant at 1% ** significant at 5% * significant at 10%. Robust asymptotic standard errors are computed using influencing functions (*csdid* default). Reference period t = −1 (2020; omitted).

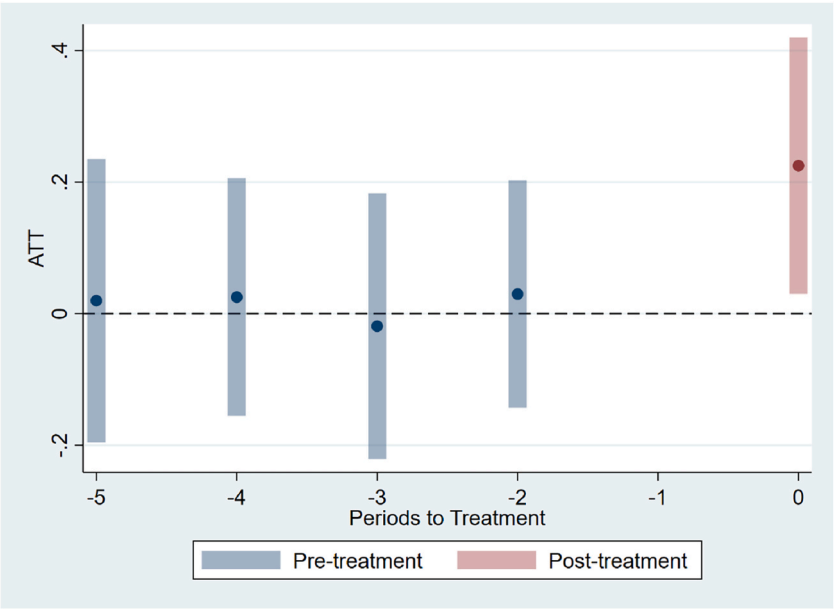


Fig. 3. The trends of the intention-to-treat effect (Model 1).

weights accounts for 11.9% of the total control group weight mass (see Appendix Table A3). The effective sample size (ESS) for the weighted controls is 636.2. This suggests that weight concentration does not appear to be substantial despite a high proportion of the control group at low propensity scores. Then, we compute standardized mean differences (SMDs) using IPW weights. As reported in Appendix Table A4, the SMDs for all covariates fell significantly after applying weights. It means that the observable covariates between the treatment and control groups were effectively balanced through DR procedure. Conditional on this covariate balance, the parallel trend assumption is satisfied in both model 1 ($\chi^2(4) = 0.3933$, p-value = 0.9830) and model 2 ($\chi^2(4) = 0.7537$, p-value = 0.9445). It means, after adjusting for covariates using the DR method, there is no statistical evidence that the trends in privacy concerns between the treatment and control groups differed before the Apple ATT was introduced. Although the treated sample is relatively small, we address major identification concerns by confirming sufficient common support to limit extrapolation, ensuring that reweighting is not dominated by extreme weights, achieving good covariate balance in the post-weight period (SMD), and finding no evidence against conditional parallel trends before treatment. Moreover, the DR estimator offers robustness if either the propensity-score or outcome model is misspecified, reinforcing the validity of our primary approach.

The results of the dynamic DID show that Apple ATT increased users' privacy concerns in the short term, consistent across both models. This pattern is consistent with prior literature suggesting that users' privacy concerns may increase when privacy interventions provide information related to the data collectors' personal data collection practices or serve as salient cues. However, as we noted

before, we interpret this empirical finding based on mechanisms discussed in the literature review section in terms of explaining the net effect of Apple ATT in the short-term, rather than inferring the relationship between the privacy concerns and certain mechanisms, because we do not measure specific variables for identifying certain mechanisms, except for privacy concerns. In this context, one possible explanation is that the observed outcomes appear to be more consistent, in the short term, with mechanisms that awaken privacy concerns than with those that relieve them. The Apple ATT requires explicit consent from eligible iOS users for third-party apps to track their personal data in iOS, and users may encounter these notices when using the app after Apple ATT takes effect, depending on their update timing and usage. In addition, the tone of the notice of third-party apps' personal data tracking practices may reflect a relatively negative framing, as noted by Baviskar et al. (2024). It implies that salient pop-up notices with a negative tone could increase users' privacy concerns in the short term, even though their primary purpose is to notify users of their right to refuse data tracking. Overall, these results support H1 as we expected. In addition, it may be interpreted that the relatively weaker result in the PC model is consistent with our underlying view of constructing the primary outcome variable, in that security dimensions and digital residues could be less related to the Apple ATT context in terms of theoretical dimensions.

4.2. The moderating effect of privacy protection literacy

In this sub-section, we investigate whether the effect of Apple ATT on users' privacy concerns is differentiated by privacy protection literacy. Based on previous literature, we employ respondents' self-reported privacy-protective digital capabilities, including awareness of protective measures and coping practices, as a proxy for privacy protection literacy (Masur, 2020; Trepte et al., 2014). In line with this context, we divide the samples in the analysis into a high literacy group and a low literacy group based on the specific value of the literacy variable.[4] Then, we implement two models in the main analysis using divided samples. The low literacy subsample includes 55 treated and 1972 control respondents, while the high literacy subsample includes 119 treated respondents and 953 control respondents. The results are summarized in Table 6.

The results show that the effect of Apple ATT is more significant for low literacy group users and the ITT effect differed significantly across groups in both models ($\chi^2(1) = 5.42$, p-value $= 0.0199$ for Model 1, $\chi^2(1) = 5.53$, p-value $= 0.0186$ for Model 2). Such a significant result in the low privacy protection literacy group can be interpreted as users who perceive that they have less knowledge about personal data protection may react more negatively when they recognize the data tracking practices via the Apple ATT. Moreover, in view of the point that general privacy literacy encompasses the knowledge of privacy protection (Park, 2013; Rosenthal et al., 2020), this result also implies that users with high privacy protection literacy, who have a possibility of understanding the context of personal data collection in advance, may not be sensitive to changes in privacy concerns stemming from the introduction of Apple ATT. This moderating effect is also consistently observed in the TWFE (Two-Way Fixed Effects) DDD (Difference-in-Difference-in-Differences) model (see Appendix Table A5). Overall, these results support H2 as we expected. It may be inferred that awakened awareness of data tracking practices and privacy-related risks may be one of the reasons why Apple ATT could increase users' privacy concerns, as previous findings suggested.

4.3. Robustness check

4.3.1. Addressing systematic differences and differential time trends

Although the pre-trend evidence and diagnostic tests support the validity of our main specification, there may still be concerns that our estimates are influenced by differential responses to common shocks unrelated to the policy, possibly due to remaining differences in observed and unobserved traits between iOS and Android users. To assess whether our results are driven by these alternative explanations, we conduct two additional analyses. First, we conduct the main analysis with the restricted subsamples: a younger cohort (born after 1991), a highly educated group (college or above as of 2020), and control respondents who had prior iPhone experience during 2016-2019. These restrictions are motivated by the fact that iOS users are, on average, younger and more educated than Android users, which may lead to systematic differences. Moreover, we view Android users with iOS experience as potentially closer to iOS users along unobserved characteristics compared to those without such experience. Results for the restricted subsamples are described in Table 7. The estimates remain consistent across all restricted subsamples. It implies that the main findings may not be driven solely by systematic differences between the two groups. Second, we conduct a TWFE DID analysis with interaction terms between all year dummy variables and key covariates (age, education level, and privacy protection literacy), using *drdid*-derived weights (summarized in Table 8). These interaction terms allow us to control for heterogeneous time trends associated with individual characteristics, including differential responses to the COVID-19 shock. For these interactions, we utilize dummy variables; *Young* dummy variable is 1 for respondents born after 1991, *High_edu* dummy variable is 1 for those with a college or above, and *High_literacy* is defined as described in Section 4.2. These results show that the TWFE DID estimates are consistent across all models. It shows that the results may not be due to varying time trends linked to these individual traits. Overall, these analyses reduce the concerns that the observed differences are mainly caused by systematic differences between the treated and control groups.

[4] We classified respondents who have more than 4 (rather than 3) of Literacy score into high literacy group because 4 means positive value in 5-Likert scale, and the average value of Literacy variable in treatment group is more than 4.

Table 6
The results of dynamic DID with the CSDID method (considering literacy).

Panel A: Model 1 (IPC)						
Event time (t)	Low literacy			High literacy		
	Coeff (Std. err)	95% CI	p-value	Coeff (Std. err)	95% CI	p-value
Pre (t = −5)	0.0244 (0.1834)	[-0.3349 0.3838]	0.8941	0.0671 (0.1391)	[-0.2056 0.3398]	0.6296
Pre (t = −4)	−0.1735 (0.1461)	[-0.4599 0.1128]	0.2350	0.1366 (0.1186)	[-0.0958 0.3691]	0.2492
Pre (t = −3)	−0.2063 (0.1659)	[-0.5315 0.1188]	0.2136	0.0943 (0.1325)	[-0.1654 0.3539]	0.4767
Pre (t = −2)	−0.1017 (0.1428)	[-0.3815 0.1782]	0.4765	0.1135 (0.1100)	[-0.1021 0.3291]	0.3021
Post (t = 0)	0.5888*** (0.1622)	[0.2708 0.9068]	0.0003	0.1105 (0.1260)	[-0.1365 0.3576]	0.3806
Obs.	12,162			6432		
Pre-trend test (p-value)	0.4408			0.7755		
Covariates	Yes			Yes		
Individual FE	Yes			Yes		
Year FE	Yes			Yes		
Panel B: Model 2 (PC)						
Event time (t)	Low literacy			High literacy		
	Coeff (Std. err)	95% CI	p-value	Coeff (Std. err)	95% CI	p-value
Pre (t = −5)	−0.0450 (0.1555)	[-0.3497 0.2597]	0.7723	0.1287 (0.1286)	[-0.1233 0.3808]	0.3167
Pre (t = −4)	−0.2152 (0.1357)	[-0.4812 0.0509]	0.1129	0.0928 (0.1116)	[-0.1259 0.3114]	0.4058
Pre (t = −3)	−0.2100 (0.1479)	[-0.4998 0.0799]	0.1556	0.1207 (0.1238)	[-0.1220 0.3634]	0.3298
Pre (t = −2)	−0.2143* (0.1240)	[-0.4573 0.0288]	0.0840	0.1057 (0.1002)	[-0.0907 0.3020]	0.2915
Post (t = 0)	0.5292*** (0.1481)	[0.2390 0.8195]	0.0004	0.0869 (0.1158)	[-0.1401 0.3140]	0.4529
Obs.	12,162			6432		
Pre-trend test (p-value)	0.1689			0.8408		
Covariates	Yes			Yes		
Individual FE	Yes			Yes		
Year FE	Yes			Yes		

Note. *** significant at 1% ** significant at 5% * significant at 10%. Robust asymptotic standard errors are computed using influencing functions (*csdid* default). Reference period t = −1 (2020; omitted). The low-literacy subsample includes 55 treated and 1972 control respondents; the high-literacy subsample includes 119 treated and 953 control respondents.

Table 7
Robustness checks for dynamic DID with the CSDID method (restricted subsamples).

	Younger subsample		High-educated subsample		Controls with prior iPhone experience	
	Coeff (Std. err)	p-value	Coeff (Std. err)	p-value	Coeff (Std. err)	p-value
Pre-average	0.1038 (0.1135)	0.3603	0.0737 (0.0866)	0.3946	0.1023 (0.0990)	0.3015
Post-average	0.2722** (0.1381)	0.0488	0.2653** (0.1064)	0.0127	0.2457** (0.1115)	0.0276
Obs.	3132		10,812		3060	
Treated individuals	105		149		174	
Controlled individuals	417		1653		336	
Pre-trend test (p-value)	0.7442		0.9158		0.7746	

Note. *** significant at 1% ** significant at 5% * significant at 10%. Robust asymptotic standard errors are computed using influencing functions (*csdid* default). Reference period t = −1 (2020; omitted). All specifications follow the baseline *csdid* setup and include the same covariates (except for the High-educated subsample analysis which did not consider education level as a covariate), individual fixed effects, and year fixed effects.

4.3.2. In-space placebo test

To assess whether our findings in the main analysis could happen randomly, given the relatively small treated sample, we conduct an in-space placebo permutation test following the previous studies' approach (Abadie et al., 2010; Bertrand et al., 2004; Chen et al., 2025; Huang & Lan, 2025). Specifically, we randomly draw a placebo-treated group (the same size as the treatment group, N = 174) from the control group and assign them the same treatment year. Then, we obtain a placebo ITT estimate by conducting the CSDID model with this placebo-treated group. By repeating this procedure 1000 times, we obtain an empirical distribution of estimated placebo coefficients as demonstrated in Fig. 4. Using a one-sided extremeness criterion, 5 out of 1000 placebo estimates are as large as the observed estimate (0.2251), corresponding to a one-sided permutation p-value of 0.006, as demonstrated in Table 9. The placebo results suggest that the findings in the main analysis are unlikely to be due to random assignment alone.

Table 8
TWFE DID estimates with controls for heterogeneous time trends (*drdid* weights).

	(1)	(2)	(3)	(4)	(5)
	Coeff (Std. err)	Coeff (Std. err)	Coeff (Std. err)	Coeff (Std. err)	Coeff (Std. err)
DID estimates					
Treated x Post	0.2069*** (0.0712)	0.2075*** (0.0709)	0.2069*** (0.0707)	0.2039*** (0.0715)	0.2058*** (0.0706)
Individual FE	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes
Young x Year FE	No	Yes	No	No	Yes
High_edu x Year FE	No	No	Yes	No	Yes
High_literacy x Year FE	No	No	No	Yes	Yes
Time-varying covariates	Yes	Yes	Yes	Yes	Yes
Obs.	18,594	18,594	18,594	18,594	18,594

Note. *** significant at 1% ** significant at 5% * significant at 10%. Standard errors are clustered at the individual level.

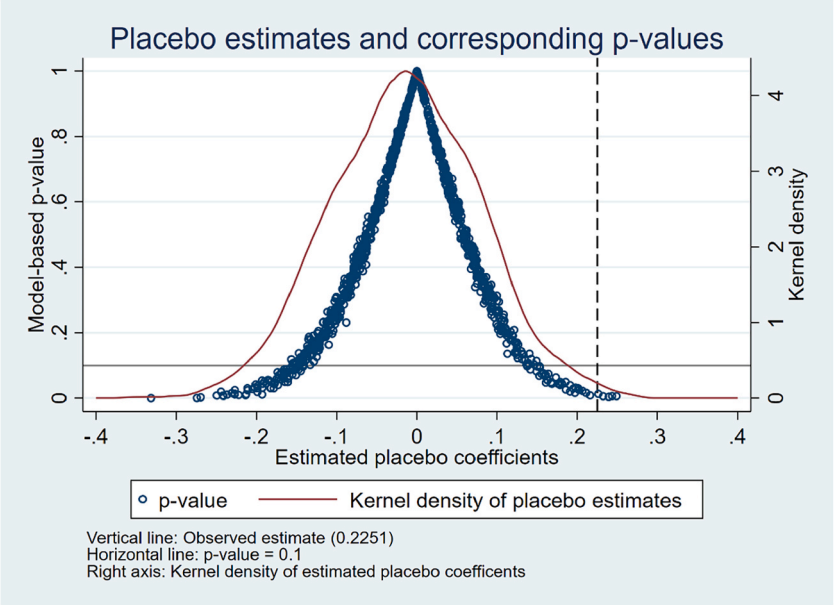


Fig. 4. In-space placebo distribution of the CSDID estimate (R = 1000).

Table 9
In-space placebo permutation test (R = 1000).

Test statistic	Observed estimates	R	Count extreme	Permutation p-value
Right-sided	0.2251	1000	5	0.0060
Two-sided			17	0.0180

Note. The permutation test is based on the main CSDID specification. Permutation p-values are computed as (Count extreme +1)/(R + 1).

4.3.3. Alternative outcome variables

Finally, we conduct the main analysis with the alternative dependent variables using items capturing the security factor (Q1, 5, 8) and digital residue factor (Q2, 3) to assess the sensitivity of our results to outcome measurement. The estimated ITT effects for these alternative outcomes (reported in Table 10) are consistent with the main findings, but the magnitudes became weaker. It can be interpreted that these weaker results are consistent with our underlying view of constructing the primary outcome variable, that those items, such as security dimensions and digital residues, could be less related to the Apple ATT context in terms of theoretical dimensions. Therefore, these results may support the content validity of our primary outcome construction, focusing on the collection dimension and general information privacy concerns.

Table 10
The results of dynamic DID with the CSDID method (alternative dependent variables).

Event time (t)	(1) security			(2) residue		
	Coeff (Std. err)	95% CI	p-value	Coeff (Std. err)	95% CI	p-value
Pre (t = −5)	0.0340 (0.1026)	[-0.1671 0.2351]	0.7405	0.1041 (0.1110)	[-0.1135 0.3217]	0.3484
Pre (t = −4)	−0.0220 (0.0883)	[-0.1952 0.1511]	0.8029	0.0060 (0.1035)	[-0.1968 0.2088]	0.9538
Pre (t = −3)	−0.0339 (0.0972)	[-0.2244 0.1566]	0.7271	0.1090 (0.1077)	[-0.1020 0.3200]	0.3113
Pre (t = −2)	−0.0518 (0.0840)	[-0.2164 0.1127]	0.5369	0.0488 (0.0962)	[-0.1399 0.2374]	0.6125
Post (t = 0)	0.1812* (0.0937)	[-0.0025 0.3649]	0.0533	0.2046* (0.1063)	[-0.0037 0.4130]	0.0543
Pre-average	−0.0185 (0.0765)	[-0.1684 0.1314]	0.8093	0.0670 (0.0865)	[-0.1026 0.2365]	0.4389
Post-average	0.1812* (0.0937)	[-0.0025 0.3649]	0.0533	0.2046* (0.1063)	[-0.0037 0.4130]	0.0543
Obs.	18,594			18,594		
Pre-trend test (p-value)	0.8936			0.7317		
Covariates	Yes			Yes		
Individual FE	Yes			Yes		
Year FE	Yes			Yes		

Note. *** significant at 1% ** significant at 5% * significant at 10%. Robust asymptotic standard errors are computed using influencing functions (*csdid* default). Reference period t = −1 (2020; omitted).

5. Conclusion

5.1. Discussions and implications

This paper investigated whether the introduction of platform-level privacy policies alleviates or increases users' privacy concerns by examining short-term changes in iOS users' privacy concerns after introducing the Apple ATT, and whether this effect is moderated by privacy protective literacy. Given that smartphone platforms are perceived as de facto privacy regulators on their platforms, we assumed that the Apple ATT, one of the representative platform-level privacy policies, could affect users' privacy concerns, either increasing or decreasing them, through mechanisms similar to those of privacy governance interventions. Specifically, however, we posited that the Apple ATT could heighten users' privacy concerns in the short-term. This is because the salient notice of data tracking may exert a stronger short-term influence on users who have become habituated to consenting to data tracking than the assurance channel implied by providing a right to refuse, partly due to negativity bias.

In the quasi-experimental setting, we found that introducing Apple ATT strengthened iOS users' privacy concerns in the short term, and this effect could be moderated by the degree of knowledge related to privacy protection and coping measures. It is meaningful that our results suggest that negative effects on users' privacy perceptions may be more salient, at least in the short term, compared to positive effects, given that Apple may have an additional incentive to frame third-party app data tracking as particularly problematic alongside protecting users' information privacy. These findings are particularly meaningful given that we use a quasi-experimental design on secondary data, rather than laboratory experiments or direct surveys, which allows us to assess the Apple ATT's short-term effect under identifying assumptions in a naturalistic setting with reduced demand effects, while also strengthening internal validity through a doubly robust method and robustness checks. Based on the literature, our findings also suggest potential mechanisms that warrant consideration in future research. One possibility is that iOS users might be newly aware or re-aware of the prevalence of third-party apps' practices of tracking personal data in iOS at an early stage after the Apple ATT took effect, and they might perceive these practices more negatively due to the Apple ATT prompts (Dinev et al., 2015; Ebert et al., 2021). In the view of habituated effect during COVID-19 (Kim et al., 2024; Wu et al., 2023) and the enhanced APCO model (Dinev et al., 2015), such increased privacy concerns may also be interpreted as a cognitive recalibration whereby a salient prompt counteracts low-effort, habituated responses to repeated consent requests. Drawing on PMT in the context of information privacy (Johnston & Warkentin, 2010; LaRose & Rifon, 2007), and to the extent that privacy protection literacy enhances coping appraisals, the moderating effect of privacy protection literacy is consistent with the view that the Apple ATT serves as risk-related cues whose effect may depend on users' coping resources. Finally, it is also suggested that the privacy interventions may not be uniformly beneficial, at least in the short term. Depending on how the intervention is framed and experienced in the user interface, and on the platform context, such policies may be associated with heightened privacy concerns by making the prevalence of data collection and tracking more salient rather than providing reassurance, particularly in the initial stage.

This study also provides some policy and managerial implications. First, the fact that the Apple ATT could increase users' privacy concerns in the short-term may be interpreted in two ways. From a negative perspective, it may suggest that users perceive data tracking practices more negatively, with heightened privacy concerns as one manifestation of this perception. However, these concerns may not be directly linked to specific behaviors, given the privacy paradox. From a positive perspective, these increased privacy concerns may reflect a consequence of recalibrating cognition about data tracking practices, where the prevalence of data tracking may be underestimated in a digital society where the use of digital services and consent to data tracking are prevalent and habituated. It implies that the effect of privacy interventions on users may not be easy to assess solely in terms of short-term changes in privacy concerns, even though such interventions are accompanied by short-term increases in privacy concerns. Therefore, it suggests that policymakers need to investigate existing users' privacy perceptions comprehensively, given the prevalence of digital services, to assess

the perceptual effect of platform-level privacy policies, including the Apple ATT, on users. Second, the point that users with a relatively high degree of literacy about information privacy protection are less sensitive to the effect of Apple ATT implies that privacy protection literacy may be an important factor in shaping users' privacy perceptions in the digital society, where privacy governance interventions and privacy-related negative events, such as data leakages and breaches, serve as risk-related cues. Therefore, it is recommended that ways be considered to enhance privacy literacy to prevent escalating users' privacy concerns unnecessarily in a regulatory environment of heightened attention to personal data protection. Thirdly, it is advisable that from the perspective of data collectors that need to comply with platform-level privacy policies and personal data protection regulations, they consider approaches to minimizing negative privacy perceptions, that may arise when salient notices foreground privacy risks, for example, by explaining more clearly how users' personal data will be better protected by complying with the privacy policies and regulations rather than simply providing minimum information which they required. Finally, although our study focuses on the short-term effect, it is worth discussing the potential long-term implications derived from our findings. On the one hand, focusing on the point that building trustworthiness takes time and users may become habituated to repeated Apple ATT notices, the heightened privacy concerns may be decreased to their original level or less over time. On the other hand, considering that periodical notice, triggered when users download new apps or update tracking policies, may repeatedly bring data tracking practices back into attention, the heightened privacy concerns may persist. Therefore, the key question is how users perceive privacy interventions like Apple ATT depending on situational contexts and individual characteristics. In this regard, as we noted previously, understanding the users' privacy perceptions and behaviors comprehensively, and enhancing various dimensions of privacy literacy can be important for relevant bodies, and their importance is not limited to the short-term.

5.2. Limitations and further scope

This study has some limitations. Firstly, the sample size of the treatment group is relatively small compared to that of the control group. Although our empirical findings are statistically significant at the 5% level, and these findings are consistent across various robustness checks, including restricted subsample sets, in-space placebo tests, and additional diagnostic checks, caution is warranted. Therefore, we suggest that our findings should be interpreted as suggestive evidence. Second, this study did not account for the heterogeneous exposure to the Apple ATT prompt, which may vary depending on updating behaviors and mobile app usage patterns, given that our main interest is the intention-to-treat (ITT) effect of the introduction of Apple ATT on iOS users. In addition, we viewed that this approach may yield attenuated estimates toward zero insofar, as including iOS users less likely to be exposed to the Apple ATT prompt may serve to dilute the net effect. Nevertheless, future studies that clearly distinguish the effect of actual exposure to the prompt would contribute to identifying the causal mechanism between privacy interventions and privacy concerns. Third, due to the inherent limitations of secondary data, this study was constrained in empirically testing the potential mechanisms discussed in the literature review. Future studies that directly measure the mediating variables, such as trustworthiness and awareness, along with privacy concerns, before and after the introduction of privacy interventions, would significantly contribute to identifying the causal relationships and mechanisms through which privacy interventions affect users' privacy perceptions in specific situational contexts and individual characteristics. Lastly, it is necessary to be cautious when generalizing our empirical findings to other gatekeeper platforms, given the distinct characteristics of Apple ATT. However, our results may still offer useful insights for understanding gatekeepers' privacy policies in settings where gatekeeper platforms act as de facto regulators within their ecosystem and operate under strategic incentives that are broadly comparable to those of Apple.

CRediT authorship contribution statement

Sangjun Nam: Writing – review & editing, Writing – original draft, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Youngsun Kwon:** Writing – review & editing, Writing – original draft, Methodology, Conceptualization.

Declaration of competing interest

None.

Acknowledgments

This article is derived from the first author's doctoral dissertation ((A) study on the relationship between personal data protection regulations and users' privacy perceptions, KAIST, 2025). An earlier version was presented at the 24th Biennial Conferenece of the International Telecommunications Society (ITS 2024 Seoul).

Appendix

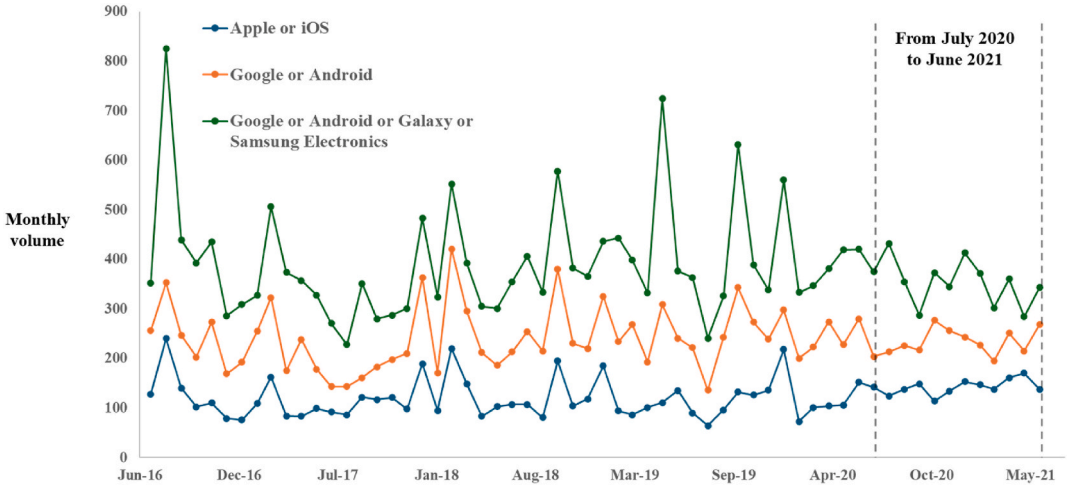


Fig. A1. Comparative trends of privacy, personal data, and security-related news by mobile ecosystem.
Note. Data retrieved from the *BigKinds* platform operated by the Korea Press Foundation (https://www.bigkinds.or.kr/). The graph compares the monthly volume of privacy-, personal data-, and security-related news across three keyword groups: (1) Apple/iOS, (2) Google/Android, (3) Google/Android/Samsung/Galaxy, from July 2016 to June 2021. Only articles categorized under IT and science were included in the analysis. Compared to previous trends, we do not observe any distinct pattern across mobile platforms that would explain a differential decline in privacy concerns among Android users in South Korea. We acknowledge that the Android/Galaxy ecosystem experienced some privacy and security developments during the post-treatment period. However, these were predominantly general updates or routine patches rather than a discrete and salient policy change such as Apple ATT.

Table A1
Propensity score distribution for treatment and control groups (based on 2020).

Propensity score range	Control group	Treatment group
0.0 – 0.1	2485 (84.96%)	54 (31.03%)
0.1 – 0.2	248 (8.48%)	37 (21.26%)
0.2 – 0.3	131 (4.48%)	41 (23.56%)
0.3 – 0.4	47 (1.61%)	27 (15.52%)
0.4 – 0.5	14 (0.48%)	12 (6.90%)
0.5 – 0.6	0 (0.00%)	3 (1.72%)
Total	2925 (100.00%)	174 (100.00%)

Note. Propensity scores are derived from *drdid*.

Table A2
Number of observations on and off the common support region (based on 2020).

	On-support	Off-support
Treatment Group	2624 (89.71%)	301 (10.29%)
Control Group	171 (98.28%)	3 (1.72%)

Note. Propensity scores are derived from *drdid*. The common support region is the intersection of the propensity score ranges for the treated and control groups.

Table A3
Distribution of propensity score weights for the control group (based on 2020).

	Min	1%	5%	25%	50%	75%	95%	99%	Max
Weight	0.0004	0.0007	0.0013	0.0050	0.0153	0.0521	0.2882	0.5589	0.9865

Note. Weights for the control group are derived from *drdid*.

Table A4
Standardized Mean Difference between treatment and control groups (based on 2020).

Variable	SMD_unweighted	SMD_weighted
Literacy	0.8574	0.0279
Gender	0.2576	−0.0028
Age	−1.4538	−0.0113
Residential area	0.1636	−0.0071
Education level	0.6875	0.0069
Monthly income	−0.2267	−0.0194
Exp	0.2580	0.0515

Table A5
TWFE DID/DDD estimates of moderation by privacy protection literacy

	(1)	(2)
	Coeff (Std. err)	Coeff (Std. err)
DID estimates		
Treated x Post	0.5178*** (0.1158)	1.3356*** (0.3244)
DDD estimates		
Treated x Post x Literacy (dummy)	−0.4691*** (0.1469)	-
Treated x Post x Literacy (continuous)	-	−0.2723*** (0.0792)
Individual FE	Yes	Yes
Year FE	Yes	Yes
Literacy x Post Control	Yes	Yes
Time-varying covariates	Yes	Yes
Weights	Yes	Yes
Obs.	18,594	18,594

Note. *** significant at 1% ** significant at 5% * significant at 10%. Standard errors are clustered at the individual level. In this analysis, *drdid*-derived weights are used, and both dummy (consistent with the subgroup analysis in Section 4.2) and continuous variables are considered in the DDD specification.

Data availability

The authors do not have permission to share data.

References

Abadie, A., Diamond, A., & Hainmueller, J. (2010). Synthetic control methods for comparative case studies: Estimating the effect of California's tobacco control program. *Journal of the American Statistical Association, 105*(490), 493–505. https://doi.org/10.1198/jasa.2009.ap08746

Angrist, J. D., & Pischke, J. S. (2009). *Mostly harmless econometrics: An empiricist's companion*. Princeton university press.

Apple. (2021). A day in the life of your data: A father-daughter day at the playground. https://www.apple.com/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf.

Baek, Y. M. (2014). Solving the privacy paradox: A counter-argument experimental approach. *Computers in Human Behavior, 38*, 33–42. https://doi.org/10.1016/j.chb.2014.05.006

Bauer, P. C., Gerdon, F., Keusch, F., Kreuter, F., & Vannette, D. (2022). Did the GDPR increase trust in data collectors? Evidence from observational and experimental data. *Information, Communication & Society, 25*(14), 2101–2121. https://doi.org/10.1080/1369118X.2021.1927138

Baviskar, S., Chowdhury, I., Deisenroth, D., Li, B., & Sokol, D. D. (2024). ATT vs. personalized ads: User's data sharing choices under apple's divergent consent strategies. *USC CLASS Research Paper No. 24-26*. Available at: SSRN 4887872 https://ssrn.com/abstract=4887872.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 1017–1041. https://doi.org/10.2307/41409971

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems, 11*(3-4), 245–270. https://doi.org/10.1016/S0963-8687(02)00018-5

Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2017). An empirical test of an Antecedents–Privacy Concerns–Outcomes model. *Journal of Information Science, 43*(5), 583–600. https://doi.org/10.1177/0165551516653590

Bergmann, M. (2008). Testing privacy awareness. In *IFIP summer school on the future of identity in the information society* (pp. 237–253). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-03315-5_18.

Bertrand, M., Duflo, E., & Mullainathan, S. (2004). How much should we trust differences-in-differences estimates? *Quarterly Journal of Economics, 119*(1), 249–275. https://doi.org/10.1162/003355304772839588

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online behavioral advertising: A literature review and research agenda. *Journal of advertising, 46*(3), 363–376. https://doi.org/10.1080/00913367.2017.1339368

Callaway, B., & Sant'Anna, P. H. (2021). Difference-in-differences with multiple time periods. *Journal of Econometrics, 225*(2), 200–230. https://doi.org/10.1016/j.jeconom.2020.12.001

Chen, Q., Qi, J., & Yan, G. (2025). Didplacebo: Stata module for in-time, in-space and mixed placebo tests for estimating difference-in-differences (did) models. https://EconPapers.repec.org/RePEc:boc:bocode:s459225.

Cheyre, C., Leyden, B. T., Baviskar, S., & Acquisti, A. (2023). The impact of apple's app tracking transparency framework on the app ecosystem. CESifo Working Paper. No. 10456 https://hdl.handle.net/10419/279205.

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. *Journal of Computer-Mediated Communication, 21*(5), 368–383. https://doi.org/10.1111/jcc4.12163

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research commentary—informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box. *Information Systems Research, 26*(4), 639–655. https://doi.org/10.1287/isre.2015.0600

Earp, J. B., & Baumer, D. (2003). Innovative web use to learn about consumer behavior and online privacy. *Communications of the ACM, 46*(4), 81–83. https://doi.org/10.1145/641205.641209

Ebert, N., Alexander Ackermann, K., & Scheppler, B. (2021). Bolder is better: Raising user awareness through salient and concise privacy notices. In *Proceedings of the 2021 CHI conference on human factors in computing systems* (pp. 1–12). https://doi.org/10.1145/3411764.3445516

Fox, G., Clohessy, T., van der Werff, L., Rosati, P., & Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behavior, 121*, Article 106806. https://doi.org/10.1016/j.chb.2021.106806

Fox, G., Lynn, T., & Rosati, P. (2022). Enhancing consumer perceptions of privacy and trust: A GDPR label perspective. *Information Technology & People, 35*(8), 181–204. https://doi.org/10.1108/ITP-09-2021-0706

Geradin, D., Katsifis, D., & Karanikioti, T. (2021). Google as a de facto privacy regulator: analysing the Privacy Sandbox from an antitrust perspective. *European Competition Journal, 17*(3), 617–681. https://doi.org/10.1080/17441056.2021.1930450

Hann, I. H., Hui, K. L., Lee, S. Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems, 24*(2), 13–42. https://doi.org/10.2753/MIS0742-1222240202

Huang, Y., & Lan, M. (2025). Network infrastructure and corporate development: A dual perspective on corporate social responsibility performance and productivity performance. *Telecommunications Policy*. , Article 103127. https://doi.org/10.1016/j.telpol.2025.103127

Ito, T. A., Larsen, J. T., Smith, N. K., & Cacioppo, J. T. (1998). Negative information weighs more heavily on the brain: The negativity bias in evaluative categorizations. *Journal of personality and social psychology, 75*(4), 887. https://doi.org/10.1037/0022-3514.75.4.887

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies, 63*(1-2), 203–227. https://doi.org/10.1016/j.ijhcs.2005.04.019

John, L. K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research, 37*(5), 858–873. https://doi.org/10.1086/656423

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 549–566. https://doi.org/10.2307/25750691

Ke, T. T., & Sudhir, K. (2023). Privacy rights and data security: GDPR and personal data markets. *Management Science, 69*(8), 4389–4412. https://doi.org/10.1287/mnsc.2022.4614

Kim, K., Maliphol, S., Shim, D., & Lee, C. (2024). Exploring the interplay between social distancing, innovation adoption, and privacy concerns amid the COVID-19 crisis. *Science and Public Policy, 51*(6), 1257–1266. https://doi.org/10.1093/scipol/scae024

Kollnig, K., Shuba, A., Van Kleek, M., Binns, R., & Shadbolt, N. (2022). Goodbye tracking? Impact of iOS app tracking transparency and privacy labels. In *In proceedings of the 2022 ACM conference on fairness, accountability, and transparency* (pp. 508–520). https://doi.org/10.1145/3531146.3533116

Kramer, J. (2025). Balancing privacy and platform power in the Mobile ecosystem: The case of apple's app tracking transparency. Available at: SSRN 5187264 https://ssrn.com/abstract=5187264.

Ksoll, C., Lilleør, H. B., Lønborg, J. H., & Rasmussen, O. D. (2016). Impact of Village Savings and Loan Associations: Evidence from a cluster randomized trial. *Journal of Development Economics, 120*, 70–85. https://doi.org/10.1016/j.jdeveco.2015.12.003

LaRose, R., & Rifon, N. (2006). Your privacy is assured-of being disturbed: Websites with and without privacy seals. *New Media & Society, 8*(6), 1009–1029. https://doi.org/10.1177/1461444806069652

LaRose, R., & Rifon, N. J. (2007). Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs, 41*(1), 127–149. https://doi.org/10.1111/j.1745-6606.2006.00071.x

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication, 8*(2), 258–269. https://doi.org/10.17645/mac.v8i2.2855

Moore, R. S., Moore, M. L., Shanahan, K. J., & Mack, B. (2015). Creepy marketing: Three dimensions of perceived excessive online privacy violation. *Marketing Management Journal, 25*(1), 42–53.

Nooren, P., Van Gorp, N., van Eijk, N., & Fathaigh, R.Ó. (2018). Should we regulate digital platforms? A new framework for evaluating policy options. *Policy & Internet, 10*(3), 264–301. https://doi.org/10.1002/poi3.177

Ozdemir, Z. D., Jeff Smith, H., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems, 26*(6), 642–660. https://doi.org/10.1057/s41303-017-0056-z

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Pew Research Center. (2019). Americans and privacy: Concerned, confused and feeling lack of control over their personal information. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

PIPC, & KISA. (2023). Survey on the personal information protection & usage (in Korean) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS273&mCode=D070020010&nttId=8726.

Rifon, N. J., LaRose, R., & Choi, S. M. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *Journal of Consumer Affairs, 39*(2), 339–362. https://doi.org/10.1111/j.1745-6606.2005.00018.x

Rios-Avila, F., Sant'Anna, P., & Callaway, B. (2023). CSDID: Stata module for the estimation of difference-in-difference models with multiple time periods. https://ideas.repec.org/c/boc/bocode/s458976.html.

Rios-Avila, F., Sant'Anna, P., & Naqvi, A. (2022). DRDID: Stata module for the estimation of doubly robust difference-in-difference models. https://EconPapers.repec.org/RePEc:boc:bocode:s458977.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rosenthal, S., Wasenden, O. C., Gronnevet, G. A., & Ling, R. (2020). A tripartite model of trust in Facebook: Acceptance of information personalization, privacy concern, and privacy literacy. *Media Psychology, 23*(6), 840–864. https://doi.org/10.1080/15213269.2019.1648218

Rozin, P., & Royzman, E. B. (2001). Negativity bias, negativity dominance, and contagion. *Personality and Social Psychology Review, 5*(4), 296–320. https://doi.org/10.1207/S15327957PSPR0504_2

Sant'Anna, P. H., & Zhao, J. (2020). Doubly robust difference-in-differences estimators. *Journal of Econometrics, 219*(1), 101–122. https://doi.org/10.1016/j.jeconom.2020.06.003

Schaub, F., Marella, A., Kalvani, P., Ur, B., Pan, C., Forney, E., & Cranor, L. F. (2016). Watching them watching me: Browser extensions' impact on user privacy awareness and concern. In *In NDSS workshop on useable security* (p. 10). https://doi.org/10.14722/usec.2016.23017

Singer, E., Hippler, H. J., & Schwarz, N. (1992). Confidentiality assurances in surveys: Reassurance or threat? *International Journal of Public Opinion Research, 4*(3), 256–268. https://doi.org/10.1093/ijpor/4.3.256

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 989–1015. https://doi.org/10.2307/41409970

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 167–196. https://doi.org/10.2307/249477

Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resources Management, 8*(3), 349–411.

Stucke, M. E. (2018). Should we be concerned about data-opolies? *Georgetown Law Technology Review, 2*(2), 275–324. https://georgetownlawtechreview.org/should-we-be-concerned-about-data-opolies/GLTR-07-2018.

Stucke, M. E., & Ezrachi, A. (2016). When competition fails to optimize quality: A look at search engines. *Yale Journal of Law and Technology, 18*(1), 70–110. http://hdl.handle.net/20.500.13051/7806.

Swani, K., Milne, G. R., & Slepchuk, A. N. (2021). Revisiting trust and privacy concern in consumers' perceptions of marketing information management practices: Replication and extension. *Journal of Interactive Marketing, 56*(1), 137–158. https://doi.org/10.1016/j.intmar.2021.03.001

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2014). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale"(OPLIS). In *Reforming European data protection law* (pp. 333–365). Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-94-017-9385-8_14.

Tucker, C. E. (2012). The economics of advertising and privacy. *International Journal of Industrial Organization, 30*(3), 326–329. https://doi.org/10.1016/j.ijindorg.2011.11.004

Van Hoboken, J., & Fathaigh, R.Ó. (2021). Smartphone platforms as privacy regulators. *Computer Law & Security Review, 41*, Article 105557. https://doi.org/10.1016/j.clsr.2021.105557

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems, 7*(6), 415–444. https://doi.org/10.17705/1jais.00092

Wang, S., Beatty, S. E., & Foxx, W. (2004). Signaling the trustworthiness of small online retailers. *Journal of Interactive Marketing, 18*(1), 53–69. https://doi.org/10.1002/dir.10071

Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior, 28*(3), 889–897. https://doi.org/10.1016/j.chb.2011.12.008

Wu, D., Min, C., Li, Z., & Wang, Y. (2023). Vigilance and habituation: Polymorphic experience effects in internet users' privacy disclosure decisions. *Decision Support Systems, 170*, Article 113961. https://doi.org/10.1016/j.dss.2023.113961

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 1.