

Fayetteville State University

DigitalCommons@Fayetteville State University

Faculty Working Papers from the School of
Business and Economics

Accounting, Finance, Healthcare Administration,
and Information Systems

2022

The Effect of Third-Party Tracking Cookies on Online Purchase Behavior: A Conceptual Model

Hamid Abbassi

Fayetteville State University

Follow this and additional works at: https://digitalcommons.uncfsu.edu/sbe_faculty_wp



Part of the [Marketing Commons](#)

Recommended Citation

Sanaei, Fariba; Abbassi, Hamid. AMA Summer Academic Conference Proceedings. 2022, Vol. 33, p486-497. 12p. , Database: Business Source Complete

This Article is brought to you for free and open access by the Accounting, Finance, Healthcare Administration, and Information Systems at DigitalCommons@Fayetteville State University. It has been accepted for inclusion in Faculty Working Papers from the School of Business and Economics by an authorized administrator of DigitalCommons@Fayetteville State University. For more information, please contact ltreadwell@uncfsu.edu.

**THE EFFECT OF THIRD-PARTY TRACKING COOKIES ON ONLINE PURCHASE
BEHAVIOR: A CONCPETUAL MODEL**

Fariba Sanaei, University of Central Florida

Hamid Abbassi, Fayetteville State University

For further information, please contact Hamid Abbassi, Assistant Professor of Marketing,
Fayetteville State University (habbassi@uncfsu.edu).

Keywords: Tracking Cookies, Perceived Risk, Online Trust, Online Retailors.

The paper explores how the use of 3rd party tracking cookies affects online trust and perceived risk, and in turn online shopping behavior.

ABSTARCT

This paper explores how the use of 3rd party tracking cookies affects online trust and perceived risk, and in turn online shopping behavior. Moreover, it is proposed that product category and country of origin moderate the effect of 3rd-party cookies on perceived risk and online trust, respectively.

INTRODUCTION

The popularity of online shopping is not hidden to anybody in a time when our lives are dominated by the internet. Based on the Market Analysis Report, the market size of world B2C e-commerce in 2020 was valued at \$3.67 trillion, and it is estimated to increase by 9.7% per year to 2028 (Market Analysis Report, 2021). In 2040, up to 95% of customer purchases will be made online (Dautovic, 2021).

On the other hand, digital advertising is growing at an impressive speed, and it is predicted that around 375 million dollars will be spent in this industry. For example, Google Ads and Facebook hold a 38.6% and 19.9% share of online advertising in the US, respectively (Smith, 2021). The effectiveness of such advertisements would be greater if they offered value to the right audience, and marketers are able to approach this targeting by collecting the consumers' online behavior data.

Since we live in a world running by data, the life is more dependent on technologies and strategies which are tracking and analyzing the information of different life aspects. within this metric universe (Ajana 2020), the use of cookies for data gathering has become favorable. For delivering the ads to right viewers. Some of the consumers are convenient with sharing their data,

whereas others are doubtful about that, for example millennials, are willing to share their data for deals, points, or discounts (G. Sterling, 2014).

Adopting tracking cookies can be beneficial for both users and online shoppers like providing personalized content and ads for users leading to better user experience, however, there are criticisms on cookies because of the amount of information and data cookies they collect. Understanding the cookies' process of gathering and analyzing data is necessary; however, it is websites responsibilities to provide a regulation for clarifying this matter. Under the General Data Protection Regulation (GDPR), site owners should make sure that the process of data gathering does not take place before the users' agreement.

First party and third-party cookies are the two main types of cookies. First-party cookies are the ones operated by the website itself. Third-party cookies are usually created by websites other than the home website, like advertisers. First-party cookies are the ones that are automatically accepted, like Google Analytics cookies, while users must accept third-party cookies because of the amount of information and data they gather for advertising networks like Facebook pixels. 56% of websites using cookies had failures in their observation, and it is predicted that this number is going to increase because of the increasing popularity of cookies and their lack of data-carrying transparency (Shaverdian 2019).

While online purchasing could provide multiple benefits, online platforms must afford the costs of customer trust and uncertainty from the point of visiting the website to the time of purchasing services like returning. The world is struggling with a trust crisis. Based on Gartner reports, in 2019, consumer trust in brands decreased by 19% compared to the 2016 rate, and this fall rate was around 33% for large companies. Covid also adds more importance to considering the process of gathering personal information from consumers.

Data violations usually take place in different industries worldwide. There are comprehensive lists of such breaches' examples. Personal information from 145.5 million Equifax customers, for example, revealed their social security numbers and credit card numbers (Ragan 2016).

In a survey project run by Pew Internet and American Life, participants were asked to share their personal information for the permission to use a website, and the results showed that 54% of the participants preferred to provide their real information as an entrance for a trade-off with internet companies. However, around 54% of users believe that online tracking has its disadvantages because it invades their privacy (Lenhart and Madden 2007).

Individuals supporting cookies believe that since cookies provide relevant ads to users, it would result in customer satisfaction. It is also argued that cookies reduce the cost of mass marketing for business owners. These advocates believe that by optimizing the amount of information and the usefulness of advertisements, online data tracking becomes meaningful (Lenhart and Madden 2007).

This paper sets some overreaching goals. First, this paper provides a comprehensive model of online customer trust, risk, and purchase behavior in online shopping stores. Second, it suggests that to what extent online businesses using 3rd-party cookies can lower their risk perceptions to enhance users' purchase behavior and how to adopt trust-building strategies into their websites. Third, this study examines how the levels of relationships between customer trust and perceived risk change with the type of personal information collected from users (health and medical data or clothing taste). Fourth, it investigates whether customers' trust in online shopping websites from their own country or international websites influences the disclosure of their personal data.

THEORITICAL BACKGROUND AND PROPOSITIONS

Our conceptual model of the role of consumers' trust in online retailers using 3rd-party tracking cookies is represented is shown in figure 1. Our model is developed from Prospect theory, Calculus theory, social exchange theory, perceived risk framework, online trust framework, and customers' intention behavior.

Online purchases are usually determined with risk and uncertainty for users. If it involves publishing their personal information with 3rd-party cookies, then their online behavior would be different. Prospect Theory provides a fundamental explanation for user decisions when the situation involves risk and uncertainty (Kahneman and Tversky 2013). Based on this theory, certain positive outcomes are more favorable for users than probable ones. It is consistent with customers' risk-aversion when making online purchases. With the popularity of online shopping, disclosure of gathered data from users has become an important matter which augments privacy issues as a consequent (Esmailzadeh 2020).

Online Trust

Based on Privacy Calculus Theory, risk and benefit exchange is usually occurred when users are trying to decide to what extend they prefer to share their data and information (Pentina et al. 2016). This trade-off is supported by Social Exchange Theory either that users tend to disclose their personal information if they think the is going to profitable (Dinev and Hart 2006) which in e-commerce settings is related to the users' privacy worries for a detriment when it comes to share their data (Gong et al., 2020). If the information leak is associated with some certain benefits, then this privacy detriment is appropriate for online customers (Bhattacharjee 2002). This behavior is considered as Privacy Paradox which can be explained by Calculus Theory (Aguirre et al., 2016). Some of this data breaches are considered as public welfare when the governments

focus on the benefits more than their risks (Nabity-Grover et al. 2020). If companies consider the gathered data as a “social contract” and propose users some benefits like higher quality services, then customers usually show tendencies for participating in this trade-off (Glazer 1991; Milne and Gordon 1993). The continuity of this participation indicates that people trust the firm overtime (Scammon and Mayer 1995).

Propensity to trust (PTT) increases customers trust so it is an important factor for online purchasing. Individuals with high propensity to trust have more tendency for doing their online purchasing since their perceived risk is much lower than the others. Studies shown that this propensity to trust is dependent to users’ culture, personal types, and experiences (Teo and Liu 2007). In short:

- **P1:** Presence of third- party tracking cookies has effects on customers’ trust.

Perceived Risk

Online trust is different and more complex when it comes to comparing it with offline trust. Online trust is an important factor for users' purchase behavior, specifically when there is a level of perceived risk for the customer (Fortes and Rita 2016). Different scholars hold different opinions about whether perceived risk has negative effects on online trust or vice versa. Scholars like Schaupp and Carter (2010) believe trust has an influence on perceived risk, while others, like Yang et al. (2015), hold the opposite attitude. In this study, term "trust" is considered as users' perception of trust for sharing their personal information and data with 3rd-party cookies when they visit an online retail website for shopping.

- **P2:** The effect of the presence of third-party tracking cookies on a customer's trust is mediated by perceived risk.

Online Purchase Intention

Given this relationship, the online purchase intention is an indicator of purchase behavior (Kim et al. 2008). In this study, we consider “perceived risk” as user’s tendency to share their personal information with 3rd-party cookies in an e-commerce context according to its possible uncertain negative outcomes. Trust is not the only reason for individuals’ online purchase behaviors; they may do their shopping without trust in a risky manner. It indicates that the positive points that customers usually perceive from the disclosure of their data, like personalized ads, can have effects on purchase intention.

Previous studies have investigated the direct effect between customers' trust and purchase behavior. In digital commerce, trust has a positive and direct effect on purchase intentions since this direct effect has been supported in multiple studies by different scholars.

- **P3:** The level of customers’ online trust affects their purchase intention.

Product Category

Privacy is defined by context (Acquisti et al. 2015), and people usually consider some types of information private in some situations but may feel comfortable sharing them in other situations. Previous research suggests that an important contextual variable in examining privacy concerns is product category (Massara et al. 2021; Segijn et al. 2021). The information shared with a hairdresser holds a different level of privacy than medical information disclosed to a health provider (Smit et al., 2021). In a framework represented by Nissenbaum (2004), it is emphasized that the product category for which data are tracked affects risk perceptions because of the different regulatory requirements.

Nowadays, most websites are collecting data from individuals for the purpose of making personalized advertisements and recommendations, which users are aware of and consider convenient (Strycharz et al. 2021). However, users' evaluation of risk varies from one product category to another. For example, while in a product category such as wearable devices, consumers report high levels of privacy concerns regarding data tracking (Pal et al. 2019), in fashion (Ariffin et al. 2018) or entertainment (Xie and Karan 2019), the increased perceived risk is not as significant. Thus, we propose the moderating effect of product category on the relationship between the use of third-party tracking cookies and perceived risk:

- **P4:** Product category moderates the effect of the use of third-party tracking cookies on perceived risk.

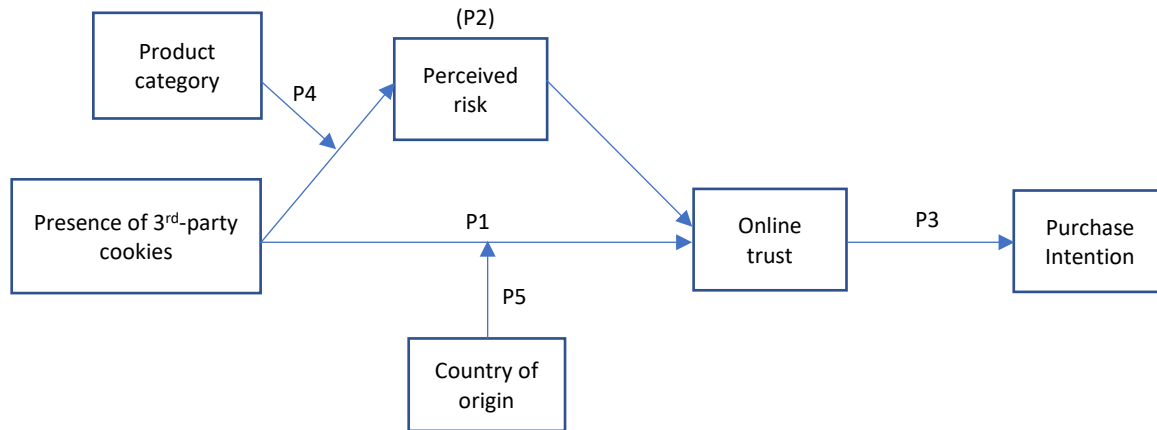
-

Country of Origin (COO)

Past research has demonstrated that COO can impact consumers' online purchase intention (Kim et al. 2017; Lee and Lee 2009). One aspect of this effect concerns the distinction between domestic versus foreign websites (Fischer and Zeugner-Roth 2017). Depending on the nationality of customers, they might have a negative perception of foreign websites (Li et al. 2020). Another aspect of the COO effect is related to the stereotypical images of countries (Janda and Rao 1997). Markos et al. (2017) showed that COO affects consumers' perceived sensitivity and their willingness to share information online. In this paper, we propose that the country of origin of the website using tracking cookies moderates the relationship between the use of third-party tracking cookies and online trust. Formally:

- **P5:** The country of origin of an online retailer moderates the effect of its use of third-party tracking cookies on online trust.

Figure 1. conceptual model



CONCLUSION

In this article, we proposed that when customers visit an online retail website that adopts 3rd-party tracking cookies, their trust level toward the website for sharing their personal information decreases in comparison to websites without cookies. This decrease in trust will affect online purchase intention. In other words, when users do not have enough trust to share their information with a website, they would rather not make a purchase either. In addition, we proposed the mediating role of risk between presence or absence of the cookies and users' trust. Furthermore, we argued that product category moderates the effect of the use of 3rd-party cookies on perceived risk. Moreover, we proposed the moderating effect of a website's country of origin on the relationship between the use of tracking cookies and online trust.

REFERENCES

- Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein (2015), "Privacy and human behavior in the age of information," *Science*, 347 (6221), 509-14.
- Ajana, Btihaj (2020), "Personal metrics: Users' experiences and perceptions of self-tracking practices and data," *Social Science Information*, 59 (4), 654-78.
- Ariffin, Shaizatulaqma Kamalul, Thenmoli Mohan, and Yen-Nee Goh (2018), "Influence of consumers' perceived risk on consumers' online purchase intention," *Journal of Research in Interactive Marketing*.
- Bhattacharjee, Anol (2002), "Individual trust in online firms: Scale development and initial test," *Journal of management information systems*, 19 (1), 211-41.
- Dinev, Tamara and Paul Hart (2006), "An extended privacy calculus model for e-commerce transactions," *Information systems research*, 17 (1), 61-80.
- Esmailzadeh, Pouyan (2020), "The impacts of the privacy policy on individual trust in health information exchanges (HIEs)," *Internet Research*.
- Fischer, Peter M and Katharina P Zeugner-Roth (2017), "Disentangling country-of-origin effects: the interplay of product ethnicity, national identity, and consumer ethnocentrism," *Marketing Letters*, 28 (2), 189-204.
- Fortes, Nuno and Paulo Rita (2016), "Privacy concerns and online purchasing behaviour: Towards an integrated model," *European Research on Management and Business Economics*, 22 (3), 167-76.
- Glazer, Rashi (1991), "Marketing in an information-intensive environment: strategic implications of knowledge as an asset," *Journal of marketing*, 55 (4), 1-19.
- Janda, Swinder and Chebrolu P Rao (1997), "The effect of country-of-origin related stereotypes and personal beliefs on product evaluation," *Psychology & Marketing*, 14 (7), 689-702.
- Kahneman, Daniel and Amos Tversky (2013), "Prospect theory: An analysis of decision under risk," in *Handbook of the fundamentals of financial decision making: Part I*: World Scientific.
- Kim, Dan J, Donald L Ferrin, and H Raghav Rao (2008), "A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents," *Decision support systems*, 44 (2), 544-64.

Kim, Namhoon, Eunha Chun, and Eunju Ko (2017), "Country of origin effects on brand image, brand evaluation, and purchase intention: A closer look at Seoul, New York, and Paris fashion collection," *International Marketing Review*.

Lee, Jin Kyun and Wei-Na Lee (2009), "Country-of-origin effects on consumer product evaluation and purchase intention: The role of objective versus subjective knowledge," *Journal of International Consumer Marketing*, 21 (2), 137-51.

Lenhart, Amanda and Mary Madden (2007), "Teens, privacy and online social networks: How teens manage their online identities and personal information in the age of MySpace."

Li, Yufan, Weichen Teng, Tien-Tien Liao, and Tom MY Lin (2020), "Exploration of patriotic brand image: its antecedents and impacts on purchase intentions," *Asia Pacific Journal of Marketing and Logistics*.

Markos, Ereni, George R Milne, and James W Peltier (2017), "Information sensitivity and willingness to provide continua: a comparative privacy study of the United States and Brazil," *Journal of Public Policy & Marketing*, 36 (1), 79-96.

Massara, Francesco, Francesco Raggiotto, and W Gregory Voss (2021), "Unpacking the privacy paradox of consumers: A psychological perspective," *Psychology & Marketing*, 38 (10), 1814-27.

Milne, George R and Mary Ellen Gordon (1993), "Direct mail privacy-efficiency trade-offs within an implied social contract framework," *Journal of Public Policy & Marketing*, 12 (2), 206-15.

Nabity-Grover, Teagen, Christy MK Cheung, and Jason Bennett Thatcher (2020), "Inside out and outside in: How the COVID-19 pandemic affects self-disclosure on social media," *International Journal of Information Management*, 55, 102188.

Nissenbaum, Helen (2004), "Privacy as contextual integrity," *Wash. L. Rev.*, 79, 119.

Pal, Debajyoti, Suree Funilkul, and Borworn Papasratorn (2019), "Antecedents of trust and the continuance intention in IoT-based smart products: The case of consumer wearables," *IEEE Access*, 7, 184160-71.

Pentina, Iryna, Lixuan Zhang, Hatem Bata, and Ying Chen (2016), "Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison," *Computers in Human Behavior*, 65, 409-19.

Ragan, Steve (2016), "412 million FriendFinder accounts exposed by hackers," Retrieved from CSO Online: <https://www.csoonline.com/article/3139311/412>

Scammon, Debra L and Robert N Mayer (1995), "Agency review of environmental marketing claims: Case-by-case decomposition of the issues," *Journal of Advertising*, 24 (2), 33-43.

Schaupp, Ludwig Christian and Lemuria Carter (2010), "The impact of trust, risk and optimism bias on E-file adoption," *Information Systems Frontiers*, 12 (3), 299-309.

Segijn, Claire M, Hilde AM Voorveld, and Khadija Ali Vakeel (2021), "The role of ad sequence and privacy concerns in personalized advertising: An eye-tracking study into synced advertising effects," *Journal of Advertising*, 50 (3), 320-29.

Shaverdian, Phillip (2019), "Start with trust: utilizing blockchain to resolve the third-party data breach problem," *UCLA L. Rev.*, 66, 1242.

Strycharz, Joanna, Edith Smit, Natali Helberger, and Guda van Noort (2021), "No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies," *Computers in Human Behavior*, 120, 106750.

Teo, Thompson SH and Jing Liu (2007), "Consumer trust in e-commerce in the United States, Singapore and China," *Omega*, 35 (1), 22-38.

Xie, Wenjing and Kavita Karan (2019), "Consumers' privacy concern and privacy protection on social network sites in the era of big data: empirical evidence from college students," *Journal of Interactive Advertising*, 19 (3), 187-201.

Yang, Qing, Chuan Pang, Liu Liu, David C Yen, and J Michael Tarn (2015), "Exploring consumer perceived risk and trust for online payments: An empirical study in China's younger generation," *Computers in Human Behavior*, 50, 9-24.

Copyright of AMA Summer Academic Conference Proceedings is the property of American Marketing Association and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.